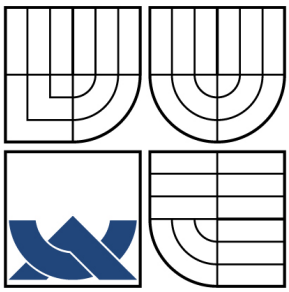
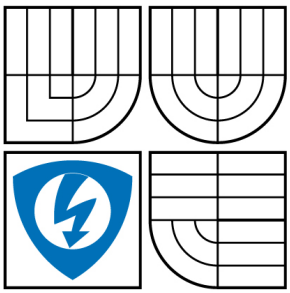


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

ANALÝZA LAN SÍTĚ S NÁSLEDNOU SIMULACÍ V PROSTŘEDÍ OPNET MODELER

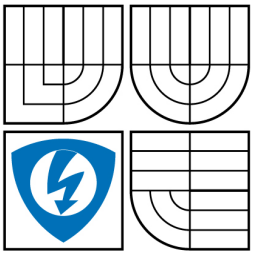
ANALYSIS OF LAN NETWORK FOLLOWED BY SIMULATION IN OPNET MODELER ENVIRONMENT

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. JAKUB SKOPAL
AUTHOR

VEDOUCÍ PRÁCE — Ing. JIŘÍ HOŠEK
SUPERVISOR

BRNO 2009



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bc. Jakub Skopal	***ID:***	83256
Ročník:	2	***Akademický rok:***	2008/2009

NÁZEV TÉMATU:

Analýza LAN sítě s následnou simulací v prostředí Opnet Modeler

POKYNY PRO VYPRACOVÁNÍ:

Prostudujte způsoby návrhu a realizace lokálních sítí. Seznamte se s možnostmi sledování a provádění analýz LAN sítí. Pomocí hardwarového síťového analyzátoru Finisar THGs proveďte komplexní analýzu vybrané LAN sítě. Výsledky analýzy použijte jako vstupní data v simulačním prostředí Opnet Modeler. Na základě těchto dat vypracujte v tomto prostředí model LAN sítě a poté proveďte simulaci, pomocí které ověřte výsledky získané z analýzy reálné sítě. Na závěr pomocí vytvořeného modelu ověřte přenosové schopnosti dané sítě.

DOPORUČENÁ LITERATURA:

[1] McCABE, J.: Network Analysis, Architecture, and Design. San Francisco: Morgan Kaufmann, 2007, ISBN: 978-0123704801.
[2] MIKALSEN, A., BORGESEN, P.: Local Area Network Management, Design & Security. Chichester: John Wiley & Sons, 2002, ISBN: 0471497695.
[3] OLIFER, N., OLIFER, V.: Computer Networks: Principles, Technologies and Protocols for Network Design. Chichester: John Wiley & Sons, 2006, ISBN: 0470869828.

Termín zadání:	9.2.2009	***Termín odevzdání:***	26.5.2009

Vedoucí práce: Ing. Jiří Hošek

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ANOTACE

Práce se zabývá prozkoumáním možností sledování a analýzy LAN sítí s využitím hardwarového analyzátoru Finisar TGHs od společnosti Finisar Corporation. Jako sledovaná síť byla vybrána lokální počítačová sít v laboratoři PA-249 na Ústavu telekomunikací, který se nachází na Vysokém učení technickém v Brně na Fakultě elektrotechniky a komunikačních technologií. V práci jsou popsány veškeré výsledky z komplexního dlouhodobého monitorování vybrané LAN sítě. Dále je práce zaměřena na simulaci a analýzu modelu této sítě v simulačním prostředí Opnet Modeler od společnosti Opnet Technologies s využitím dat získaných z dlouhodobého monitorování. Získaná data z analýzy byla použita jako podklad simulace provozu vytvořeného virtuálního modelu reálné LAN sítě. Poslední část práce popisuje ověření přenosových schopností a vlastností reálné LAN sítě. Ověření bylo provedeno v prostředí Opnet Modeler, kde byla síť podrobně zkoumána.

KLÍČOVÁ SLOVA

LAN, analýza, monitorování, analyzátor, Finisar TGHs, simulace, Opnet Modeler.

ABSTRACT

This thesis deals with the exploration of possibilities of LAN analysis with the use of the hardware analyzer Finisar TGHs from the Finisar Corporation Company. As a monitored network was choosed the local computer network in the laboratory PA-249 at the Department of Telecommunications, which is located at the Faculty of Electrical Engineering and Communication, Brno University of Technology. All results acquired from the complex long-term monitoring of the choosed LAN network are described in this thesis. Further, the thesis is focused on the simulation and analysis of the model of this network that was created in the simulation environment Opnet Modeler. The data obtained from the real LAN monitoring were used as a basis of an operating simulation of the transmission abilities and features of the real LAN network. The last part of the thesis describes the verification of the transmission capabilities and characteristics of the real LAN. Verification was performed in Opnet Modeler, where the network has been analyzed in detail.

KEYWORDS

LAN, analysis, monitoring, analyzer, Finisar TGHs, simulation, Opnet Modeler.

SKOPAL, J. *Analýza LAN sítě s následnou simulací v prostředí Opnet Modeler*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2009. 76 s. Vedoucí diplomové práce Ing. Jiří Hošek.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Analýza LAN sítě s následnou simulací v prostředí Opnet Modeler“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujícího autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne ....

Podpis autora

PODĚKOVÁNÍ

Děkuji vedoucímu diplomové práce Ing. Jiřímu Hoškovi, za velmi užitečnou metodickou pomoc a cenné rady při zpracování diplomové práce.

V Brně dne …… ……..
(podpis autora)

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

V současnosti jsou kladeny stále větší požadavky na rychlejší a kvalitnější komunikaci s okolním světem, a proto se počítačové sítě staly nezbytnou a nepostradatelnou součástí všech organizací různých velikostí. S rostoucími požadavky uživatelů a technických pracovníků se stávají stále více rozsáhlejší a komplexnější, často představují složité a rozsáhlé systémy hardwaru a softwaru a vzniklé potíže mají neblahý vliv na produktivitu stovek až tisíců uživatelů.

Na provoz reálné sítě má vliv velké množství aspektů, od vlastností pasivních i aktivních prvků, používaných komunikačních protokolů, až po samotné síťové aplikace. A proto je nutné aby správci byli schopni co nejrychleji a nejefektivněji nalézt nebo lokalizovat příčinu vzniklých problémů a zajistit tak rychlou a účinnou nápravu dané situace. K těmto účelům byly vyvinuty komplexní a všestranné nástroje pro sledování, analýzu a celkovou simulaci provozu v LAN sítích. Analyzátory umožňují krátkodobou nebo dlouhodobou analýzu činnosti sítí a dokáží tak odhalit slabá místa, ve kterých se vyskytují potíže. Bez dat získaných z analyzátorů neexistuje prakticky žádný způsob jak zjistit, co se v síti děje. Simulační nástroje nám taktéž poskytují velmi mocné a praktické nástroje pro modelování rozsáhlých informačních infrastruktur a umožňují jednoduše a snadno nasimulovat chování budoucí sítě ještě před její vlastní realizací. Pomocí těchto nástrojů jsme schopni odhalit potenciální nežádoucí problémy a stavy sítě, které by mohly nastat při běžném provozu, a snížit tak velmi vysoké náklady na zprovoznění a ladění dané infrastruktury.

Úkolem této diplomové práce bylo seznámit se základními způsoby návrhu a realizace lokálních sítí a možnostmi sledování a analýzy jejich provozu. Dále, pomocí hardwarového analyzátoru Finisar TGHs, provést dlouhodobou komplexní analýzu vybrané LAN sítě, následně vytvořit model dané sítě v simulačním prostředí Opnet Modeler a jako vstupní data použít výsledky získané z dlouhodobého monitorování vybrané sítě. Dalším úkolem této práce bylo pomocí vytvořeného modelu v Opnet Modeler ověřit přenosové schopnosti a vlastnosti analyzované sítě. Pro monitorování byla vybrána lokální počítačová síť v laboratoři PA-249 na ústavu telekomunikací. Délka analýzy a následné simulace trvala jeden týden.

V kapitole 1 jsou stručně představeny LAN sítě a jejich základní topologie. Dále je zde znázorněna architektura sady TCP/IP protokolů s rozdělením do jednotlivých vrstev.

Kapitola 2 popisuje základní způsoby a metody návrhu a realizace lokálních počítačových sítí. Jsou zde také představena dostupná přenosová média pro výstavbu strukturované kabeláže a způsoby rozdělení kabelážního systému do určitých sekcí.

Kapitola 3 v sobě zahrnuje základní popis metod pro komplexní analýzu a monitorování sítí. Dále jsou zde popsány dostupné softwarové a hardwarové nástroje a také hardwarový analyzátor Finisar TGHs.

Kapitola 4 je věnována výsledkům první dlouhodobé analýzy LAN sítě v laboratoři PA-249. Je zde charakterizován model zmíněné sítě a souhrnný výskyt nejčastěji se vyskytujících protokolů a služeb.

V kapitole 5 jsou popsány výsledky z druhého dlouhodobého monitorování stejné sítě. Dále jsou zde upřesněny výsledky, které byly následně použity jako vstupní data pro simulaci v prostředí Opnet Modeler.

Kapitola 6 se zabývá vlastní simulací modelu reálné LAN sítě v simulačním prostředí Opnet Modeler. Tato kapitola je pomyslně rozdělena do dvou hlavních částí. V první části je popsána simulace, ve které byly ověřeny výsledky získané z dlouhodobého monitorování LAN sítě. Druhá část je zaměřena především na ověření přenosových schopností a vlastností sítě. Jsou zde popsány výsledky jednotlivých simulací, které byly provedeny pro získání potřebných dat pro ověření schopností.

1. LAN SÍTĚ A RODINA PROTOKOLŮ TCP/IP

1.1. LAN sítě

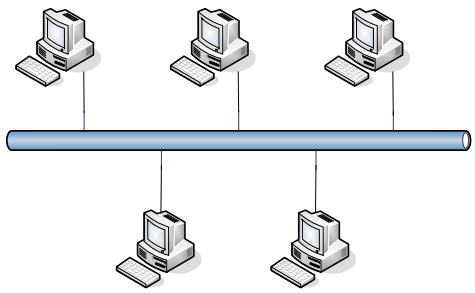
Sítě LAN (Local Area Network) jsou komunikační sítě, které propojují skupiny počítačů a dalších zařízení na omezenou vzdálenost a to uvnitř místnosti, budov, malých areálů nebo v rámci jedné organizace. Hlavními výhodami je vysoká škála přenosových rychlostí (od desítek Mbs až po desítky Gbs) při relativně nízké pořizovací ceně. LAN slouží ke snadnému sdílení informací a technických prostředků (např. diskových prostor, tiskáren, skenerů, kopírovacích zařízení apod.). [7] Dále umožňuje sdílet přístup k Internetu a k němu navázaným službám (E-mail, HTTP, FTP, Peer-to-peer sítě, apod.)

K propojení jednotlivých prvků v těchto sítích slouží směrovače a přepínače. Jako přenosové médium se používá kroucená dvojlinka UTP (Unshielded Twisted Pair) (v současné době nejpoužívanější a nejdostupnější), koaxiální kabel (zastaralé) a optická vlákna (moderní spoj, používá se na propojení vzdálených míst). [7]

1.1.1. Topologie LAN

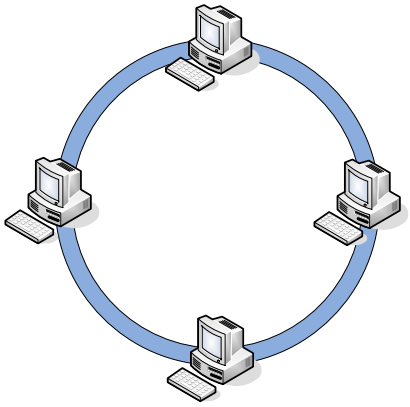
Mezi základní topologie sítí LAN patří:

Sběrnicová topologie (Bus) – tuto topologii používá Ethernet realizovaný koaxiálním kabelem. Existují dvě specifikace, 10Base-2 a 10Base-5, rozdíl je dán typem použitého kabelu a jeho délkou. [11] V dnešní době se již nepoužívá. Nevýhodou této topologie je, že při přerušení vodiče se zhroutí celá síť. Výhodou je nízká pořizovací cena a snadná realizace vysílání zpráv pro všechny stanice.



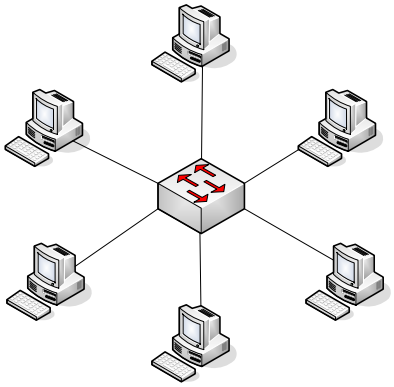
Obr. 1.1: *Sběrnicová topologie*

Kruhová topologie (Ring) – tato topologie je založena na tom, že vysílací část jednoho uzlu je zapojena do přijímací části uzlu následujícího. Typickými technologiemi používajícími topologii kruhu jsou Token Ring a FDDI (Fiber Distributed Data Interface). [11] Nevýhodou je, že při výpadku jedné stanice nastává zhroucení celé sítě. Výhodou je jednoduchá výstavba, nepotřebuje žádný centrální prvek.



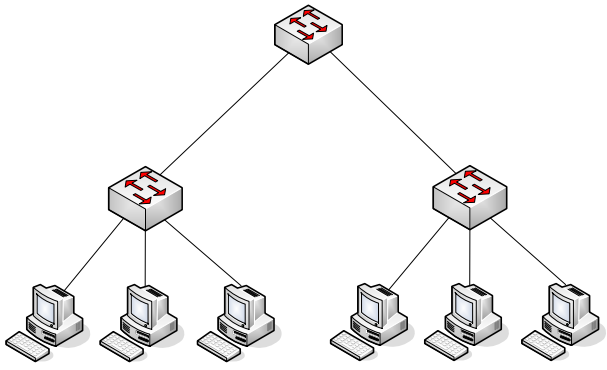
Obr. 1.2: *Kruhová topologie*

Hvězdicová topologie (Star) - v dnešní době je nejpoužívanější topologií při výstavbě nových sítí. Koncové uzly jsou propojeny s hlavním centrálním uzlem a to tak, že každý koncový uzel má svůj vlastní spoj. Předností této sítě je, že výpadek stanice nebo spoje neovlivní chod celé sítě. Nevýhodou je nutnost centrálního prvku.



Obr. 1.3: *Hvězdicová topologie*

Stromová topologie (Tree) – je zobecněná topologie „Hvězda“. Je to v podstatě spojení několika sítí s hvězdicovou topologií, jejích centrální prvky jsou spojeny. Výhodou této sítě je, že při výpadku jednoho centrálního prvku zůstává zbytek sítě funkční kromě části sítě připojené na tento prvek.



Obr. 1.4: *Stromová Topologie*

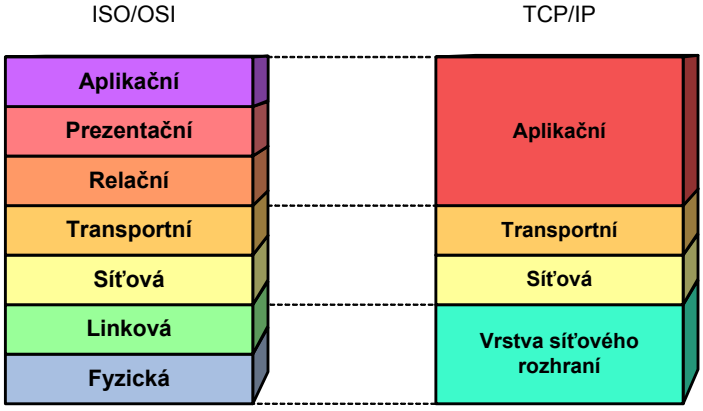
1.2. TCP/IP

Rodina protokolů TCP/IP (Transmission Control Protocol / Internet Protocol) je v dnešní době součástí všech operačních systémů a nejpoužívanější sadou protokolů v počítačových sítích i v celém Internetu. Jsou to ve skutečnosti dva zcela odlišné protokoly, které fungují v síťové vrstvě (IP) a transportní vrstvě (TCP) modelu OSI (Open Systems Interconnection). [7] TCP/IP byl vyvinut před více než dvaceti lety jako komunikační protokol ministerstva obrany USA pro sjednocení počítačové sítě ARPANET. Model TCP/IP není závislý na přenosovém médiu a může být použit v sítích WAN (Wide Area Network) i LAN, jak pro sériové linky a koaxiální kabely, tak i pro vysokorychlostní optické sítě.

1.2.1. Architektura TCP/IP

Architektura TCP/IP je založena na vrstvovém modelu (viz. Obr. 1.5), který vychází přímo z modelu ISO OSI. Každá vrstva využívá služeb nižší vrstvy a poskytuje služby vrstvě vyšší. Síťový model se skládá jen ze 4 vrstev na rozdíl od referenčního modelu OSI, jsou to:

- Aplikační vrstva (application layer)
- Transportní vrstva (transport layer)
- Síťová vrstva (internet layer)
- Vrstva síťového rozhraní (network interface)



Obr. 1.5: *Srovnání ISO/OSI a TCP/IP architektury*

Aplikační vrstva – jsou zde provozovány základní aplikace v rámci TCP/IP. Aplikační vrstva zajišťuje přenos a srozumitelnost zpráv. Aplikační vrstva v TCP/IP sdružuje 3 vrstvy z ISO/OSI a to aplikační, prezentační a relační.

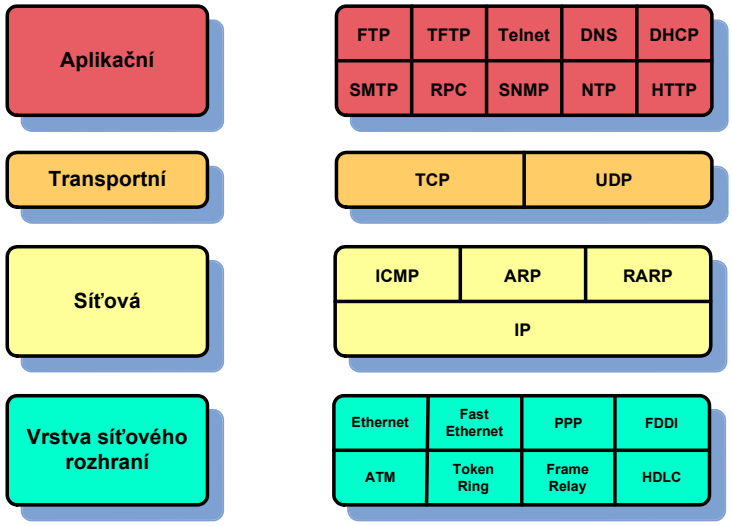
Transportní vrstva – tato vrstva odpovídá v podstatě transportní vrstvě v OSI modelu. Poskytuje mechanismy pro koncový přenos dat mezi dvěmi stanicemi. Poskytuje transportní službu se spojením TCP a transportní službu bez spojení UDP (User Datagram Protocol). [13]

Síťová vrstva – vrstva zajišťující síťovou adresaci, směřování a předávaní paketů. Síťová vrstva nepoužívá žádný spolehlivý protokol, proto se spoléhá na protokoly vyšších vrstev, že v případě ztráty paketů zajistí jejich opětovný přenos. Další funkcí je provádění segmentace a znovu sestavování paketů do a z rámců specifikovaných protokolem nižší vrstvy. [13]

Vrstva síťového rozhraní – zajišťuje přenos rámců mezi dvěma přímo propojenými uzly sítě. Jsou zde definovány metody přístupu na médium. Tato vrstva je specifická pro každou síť v závislosti na její implementaci (Ethernet, Token Ring, FDDI, X.25).

1.2.2. Sada protokolů rodiny TCP/IP

Každá rovina TCP/IP modelu využívá různé komunikační protokoly. Přehled jednotlivých protokolů je zobrazen na následujícím Obr. 1.6.

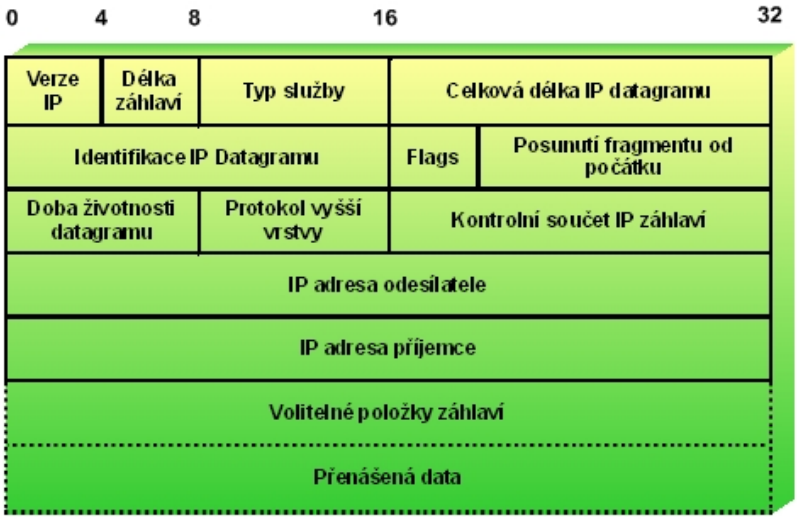


Obr. 1.6: *Zařazení protokolů do modelu TC/IP*

1.2.3. Protokoly síťové vrstvy

V této vrstvě se vyskytuje stěžejní protokol TCP/IP a to IP. Dále zde pracují protokoly ICMP (Internet Control Message Protocol) a na rozhraní s transportní vrstvou ARP (Address Resolution Protocol) a RARP (Reverse Address Resolution Protocol).

IP (Internet Protocol) – na základě síťových adres doručuje data (datagramy) přes jednotlivé uzly až ke koncovému adresátovi. IP poskytuje nespolehlivou přenosovou službu nespojového charakteru a zastává funkce adresování stanic v síťové vrstvě, definici struktury IP datagramu, propojení síťové a transportní vrstvy, fragmentaci a sestavení datagramů. [3] Každý datagram je samostatná jednotka, která obsahuje všechny informace o odesílateli a adresátovi. V dnešní době se využívají dvě verze tohoto protokolu a to verze starší IPv4 a verze novější IPv6. Na následujícím obrázku (Obr. 1.7) je zobrazen formát IP datagramu.



Obr. 1.7: *Struktura IP datagramu verze 4*

- ***Verze IP (4 bity)*** – první položka v záhlaví IP datagramu, obsahuje verzi IP protokolu. Jak již bylo zmíněno, verze protokolu může být 4 nebo 6.
- ***Délka záhlaví (4 bity)*** **–** indikuje délku záhlaví jako počet 32 bitových slov. [13]
- ***Typ služby (8 bitů)*** **–** specifikuje, jak má datagram zpracovat konkrétní protokol vyšší vrstvy z hlediska priorit. Tato položka nenašla v praxi uplatnění.
- ***Celková délka IP datagramu (16 bitů)*** **–** zde je uložená délka celého datagramu v oktetech.
- ***Identifikace IP datagramu (16 bitů)*** **–** slouží jako identifikátor odeslaného paketu, který byl fragmentován.
- ***Příznaky (3 bity)*** **–** toto pole je důležité při fragmentaci paketu. Určuje, zda může být datagram fragmentován.
- ***Posunutí fragmentu od počátku (13 bitů)*** **-** udává, na jaké pozici v původním datagramu začíná tento fragment. [14]
- ***Doba životnosti datagramu TTL (8 bitů)*** **–** počítadlo nastavené zdrojovou stanicí a při každém průchodu uzlem se tato hodnota sníží o jedničku, při dosažení nulové hodnoty se paket zahodí. Slouží jako ochrana proti zacyklení paketu.
- ***Protokol vyšší vrstvy (8 bitů)*** **–** indikuje protokol vyšší vrstvy, pro který je datagram určen.
- ***Kontrolní součet z IP záhlaví (16 bitů)*** **–** je to kontrolní součet a z hlavičky datagramu, ověřuje zda nedošlo k chybě, pokud ano paket je zahozen.
- ***IP adresa odesílatele (32 bitů)*** **–** IPv4 adresa odesílatele.
- ***IP adresa příjemce (32 bitů)*** **–** IPv4 adresa příjemce .

- ***Volitelné položky (32 bitů)* –** různé rozšiřující informace a požadavky, např. zabezpečení, dodržení předepsané cesty sítí apod..

ICMP (Internet Control Message Protocol) – slouží pro přenos chybových a řídících zpráv mezi jednotlivými uzly sítě. Své datové pakety balí do IP protokolu. Pomocí ICMP lze také sledovat propustnost a dostupnost sítě. Na následujícím obrázku (Obr. 1.8) je zobrazen ICMP datagram. [14]

Obr. 1.8: *Struktura ICMP paketu*

- ***Typ (8 bitů)*** – typ a formát zprávy ICMP.
- ***Délka záhlaví (8 bity)* –** upřesnění informace typu zprávy.
- ***Typ služby (16 bitů)* –** zabezpečení záhlaví zprávy.

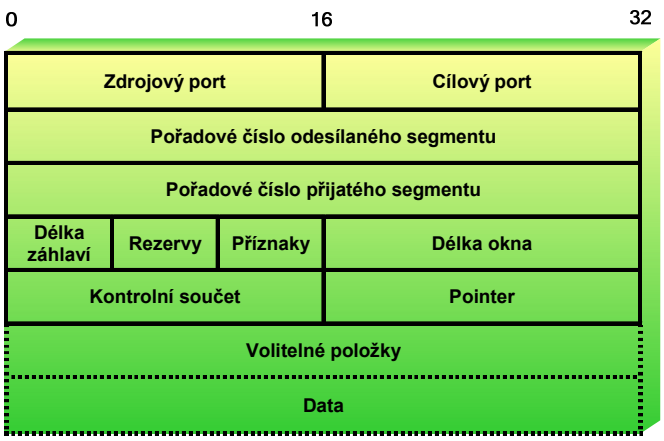
ARP (Address Resolution Protocol) – každé síťové zařízení má svou fyzickou adresu. Aby bylo možné posílat datagramy sítí, musíme znát jednak logickou (IP), tak i fyzickou (MAC) adresu uzlu. K tomu nám slouží ARP protokol. Jeho hlavní funkce spočívá v tom, že pomocí logické adresy nalezne fyzickou adresu daného zařízení.

RARP (Reverse Address Resolution Protocol) – slouží ke zjištění logické adresy uzlu při znalosti jeho fyzické adresy. Smysl protokolu RARP je u bezdiskových stanic. Bezdisková stanice po svém zapnutí nezná nic jiného než svou fyzickou adresu (tu má uloženu výrobcem v paměti ROM). Po svém zapnutí se potřebuje dozvědět svou IP adresu k tomu použije RARP protokol. [3]

1.2.4. Protokoly transportní vrstvy

Na transportní vrstvě jsou provozovány pouze dva typy protokolů TCP a UDP. Zajišťují buď spolehlivou nebo nespolehlivou službu a záleží na aplikaci, kterou z nich si vybere.

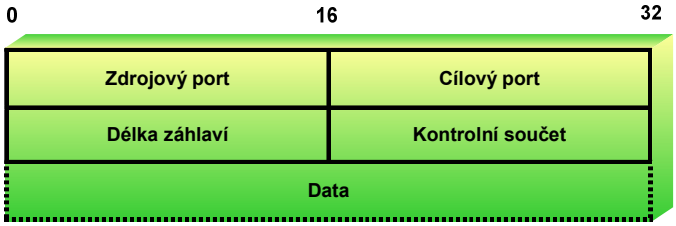
TCP (Transmission Control Protocol) – tento protokol zajišťuje spojení, navázání, udržení a ukončení spojení mezi dvěma uzly v síti. Poskytuje transportní spolehlivou spojovou službu mezi aplikacemi (tzn., že garantuje spolehlivé doručení segmentů a to ve správném pořadí). Příjemce musí potvrzovat přijímaná data, v případě ztráty dat (TCP segmentu) si vyžádá zopakování odeslání segmentu. [3] Adresou TCP protokolu je dvoubytové číslo portu, které nabývá hodnot od 0 až po 65535. Každá aplikace která komunikuje pomocí TCP má přiřazené specifické číslo (http – port 80, ftp – port 21, telnet – port 23, atd.). Struktura TCP segmentu je zobrazena na následujícím obrázku (Obr. 1.9).



Obr. 1.9: *Struktura TCP segmentu*

- ***Zdrojový port (Source Port)* - 16 bitů** – port odesílatele TCP segmentu.
- ***Cílový port (Destination Port)* – 16 bitů** – port příjemce TCP segmentu.
- ***Pořadové číslo odesílaného segmentu (Sequence Number)* – 32 bitů –** pořadové číslo TCP segmentu v toku dat od odesílatele k příjemci.
- ***Pořadové číslo přijatého segmentu (Acknowledgment Number)* – 32 bitů** – vyjadřuje číslo následujícího, který je příjemce připraven přijmout.
- ***Délka záhlaví (Leader Length)* – 4 bity –** vyjadřuje délku záhlaví TCP segmentu.
- ***Příznaky (Flags)* – 6 bitů** – nastavení příznaku TCP segmentu (URG, ACK, PSH, RST, SYN, FIN).
- ***Délka okna (Windows size)* – 16 bitů** – vyjadřuje délku okna u TCP segmentu.
- ***Kontrolní součet (Checksum)* – 16 bitů** – zabezpečení záhlaví pomocí CRC součtu.
- ***Ukazatel naléhavých dat (Urgent Pointer)* – 16 bitů –** ukazatel na konec úseku naléhavých zpráv. Odesílatel tím dává najevo aby byla tyto data přednostně zpracována.
- ***Volitelné položky (Options)* – 0 až 32 bitů** – volitelné položky TCP segmentu.

UDP (User Datagram Protokol) – na rozdíl od protokolu TCP UDP nabízí transportní nespolehlivou službu bez spojení. Nezaručuje doručení UDP datagramu sítí, odesílatel odešle UDP datagram a už se nestará, zda byl doručen, to musí zajistit aplikace. [13] Pro svou adresaci používá stejně jako TCP čísla portů. Struktura UDP datagramu je zobrazena na Obr. 1.10.



Obr. 1.10: *Struktura UDP datagramu*

- ***Zdrojový port (Source Port)* - 16 bitů** – port odesílatele UDP datagramu.
- ***Cílový port (Destination Port)* – 16 bitů** – port příjemce UDP datagramu.
- ***Délka záhlaví (Leader Length)* – 4 bity –** vyjadřuje délku záhlaví UDP datagramu.
- ***Kontrolní součet (Checksum)* – 16 bitů** – zabezpečení záhlaví pomocí CRC součtu.

1.2.5. Protokoly aplikační vrstvy

Tato vrstva zahrnuje přímo aplikace nebo procesy, které komunikují po síti a nabízejí uživatelům konkrétní služby pro přenos dat. Určité aplikační protokoly jsou přímo závislé na typu přenosové služby, proto buď vyžadují spolehlivý protokol se spojením TCP (např. telnet, FTP, apod.), nebo protokol nespolehlivý bez spojení UDP (např. SNMP, BOOTP, TFTP). Některé z protokolů však mohou používat kterýkoliv z transportních protokolů. [13] Každá síťová aplikace je specificky určena číslem portu, na kterém komunikuje. Aplikační vrstva obsahuje velké množství protokolů a nové stále vznikají, proto budou v následujícím textu uvedeny jen nejznámější z nich.

HTTP (HyperText Transfer Protocol) – protokol pro přenos hypertextových informací mezi WWW servery a jejich klienty. Je to nejvíce používaný objektově orientovaný protokol v aplikační vrstvě. Klientovi umožňuje vyžádat si na WWW serveru určitou stránku a ten mu ji pak zašle. Tento protokol je koncipován jako bezestavový, tudíž každý požadavek je samostatný, není potřeba znát předešlý nebo následující. HTTP pro svou komunikaci potřebuje protokol TCP. Je jednoznačně definován číslem portu 80. [1][3]

FTP (File Transfer Protocol) – protokol pro přenos souborů mezi serverem a klientem. FTP ke komunikaci využívá spolehlivou službu TCP a je určen portem 20 a 21.

SMTP (Simple Mail Transfer Protocol) – slouží pro komunikaci mezi e-mailovými servery a pro přenos e-mailových zpráv.

POP (Post Office Protocol) – slouží pro příjem elektronické pošty z poštovních serverů.

Telnet – protokol pro připojení ke vzdálené stanici. Umožňuje ovládat vzdálenou stanici, spouštět různé aplikace apod. Je mutliplatformní, to znamená, že není závislý na

operačním systému a proto se můžeme pomocí tohoto protokolu připojit i ke stanicím, které mají odlišný operační systém.

SNMP (Simple Network Management Protocol) – protokol sloužící potřebám správy sítí. Umožňuje průběžný sběr nejrůznějších informací pro potřeby správy sítě a jejich následné vyhodnocování. Na tomto protokolu je dnes založena většina prostředků a nástrojů pro správu sítě. [8]

DNS (Domain Name server) – protokol pro rychlý převod jmen stanic na IP adresy a naopak. Je to distribuovaný hierarchický systém, který je založen na převodních tabulkách se jmény stanic a jejich IP adres.

BOOTP (BOOTstrap Protocol) - protokol aplikační vrstvy sloužící pro získání IP adresy při startu systému. Svými funkcemi je BOOTP podobný protokolu RARP pracujícímu na hranici spojové a síťové vrstvy. Protokol BOOTP je v dnešní době nahrazen dynamickým protokolem DHCP. [13]

DHCP (Dynamic Host Configuration Protocol) – protokol, který dynamicky přiděluje stanicím v síti informace potřebné pro komunikaci (IP adresa, maska sítě, výchozí brána, DNS servery a další). Výrazně tak zjednodušuje správu sítě.

NTP (Network Time Protocol) – synchronizační protokol, slouží pro časovou synchronizaci uzlů v síti.

RTP (Real-time Transfer Protocol) – protokol pro přenosy v reálném čase, např. videa.

2. NÁVRH A REALIZACE LAN SÍTÍ

2.1. Úvod

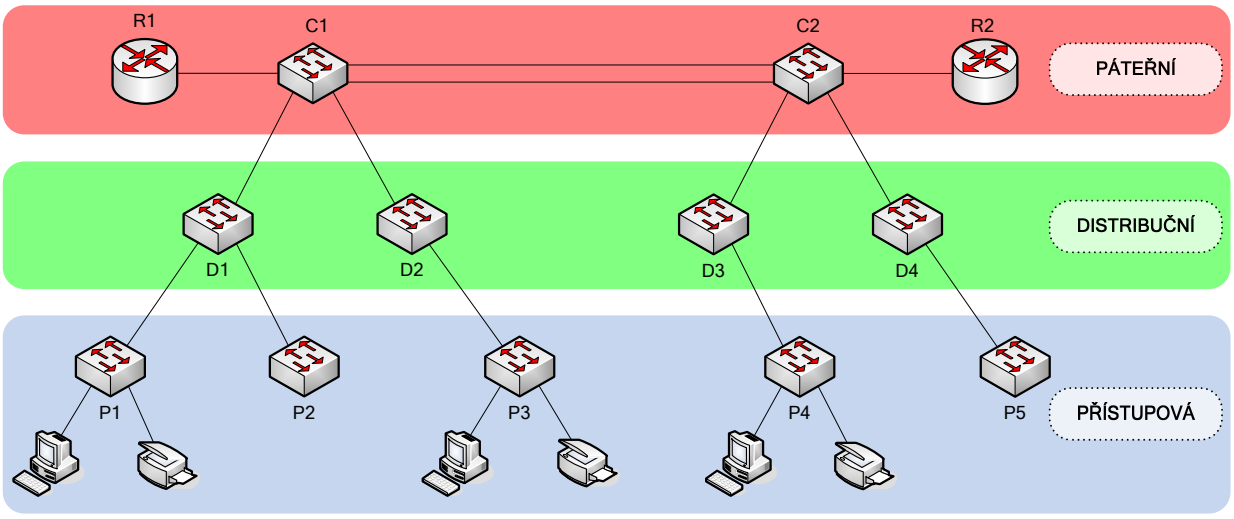
Při vytváření LAN sítí je potřeba řídit se pečlivě připraveným plánem, který je založen na celkovém pochopení zahrnutých hardwarových i softwarových prvků. Základem pro výstavbu nové, nebo modernizaci stávající sítě je nutné dobré plánování a metodický postup. Pokud se provádí inovace stávající sítě, je zapotřebí nashromáždit dostatečné informace o aktuální struktuře sítě, použitém hardwaru a kabeláži a mít přístup ke všem dokumentům. Při návrhu nové sítě je nezbytné zohlednit potřeby organizace, vybrat vhodný hardware a kabeláž, naplánovat implementaci sítě. [1]

V dnešní době firmy stále více využívají pro komunikaci digitální svět (přenos videa a hlasu pomocí internetové sítě). Proto je důležité, abychom byly schopni navrhnout LAN síť s vhodnými prvky, které spolehlivě zajistí všechny požadavky uživatelů.

2.2. Hierarchický síťový model

Při návrhu větších LAN sítí se nejčastěji využívá hierarchický síťový model. Ve srovnání s dalšími návrhy sítě je tento model nejsnazší pro řízení, umožňuje jednoduché rozšíření a vzniklé problémy jsou snadno a rychle řešitelné.

Hierarchický návrh sítě je koncept, který dělí celou sít do diskrétních vrstev. Každá vrstva poskytuje specifické funkce a definuje roli uvnitř celé sítě. [6] Typický hierarchický model se skládá ze tří vrstev: přístupová vrstva (Access Layer), distribuční vrstva (Distribution Layer) a páteřní vrstva (Core Layer). Příklad třívrstvého modelu je zobrazen na Obr. 2.1.



Obr. 2.1: *Hierarchický síťový model*

2.2.1. Přístupová vrstva

Přístupová vrstva (Access Layer) poskytuje koncovým zařízením (PC, tiskárny, IP telefony) přístup ke zbytku sítě. V této vrstvě můžou být zahrnuty i směrovače, přepínače, rozbočovače nebo bezdrátové přístupové body (AP). Hlavním cílem přístupové vrstvy je poskytnutí prostředků pro připojení koncových zařízení k sítí a kontrola povolení komunikace na síti.

2.2.2. Distribuční vrstva

Distribuční vrstva (Distribution Layer) shromažďuje data přijatá od přístupové vrstvy a předává je páteřní vrstvě, která je směruje ke koncovému bodu. Distribuční vrstva ovládá tok síťového provozu, využívá politiky a vymezuje relace mezi virtuálními lokálními sítěmi (VLAN), které jsou definované v přístupové vrstvě. VLAN umožňuje dělit síťovou komunikaci na přepínačích do separátních pomocných sítí. [6] Distribuční přepínače jsou většinou výkonná zařízení, která mají vysokou dostupnost a velké rezervy k tomu, aby zajistili dostatečnou spolehlivost a propustnost přístupové vrstvě.

2.2.3. Páteřní vrstva

Páteřní vrstva (Core Layer) hierarchického návrhu je vysokorychlostní mezisíťová páteř. Tato vrstva je kritická pro spojení zařízení na distribuční vrstvě, a proto je důležité, aby uzly páteřní vrstvy byly vysoce dostupné a měli velké rezervy pro případné rozšíření. [6] Prvky mohou být připojeny přímo do sítě internet. Páteřní vrstva shromažďuje datový tok od všech zařízení z distribuční vrstvy, a proto musí být schopna přenášet velké množství dat a to dostatečnou rychlostí.

2.2.4. Výhody hierarchického modelu

Hierarchické řešení návrhu rozsáhlejších LAN má mnoho výhod a proto je tento návrh často využíván. Největšími přednostmi jsou:

- **Rozšiřitelnost** – tyto sítě díky své modularitě nabízejí jednoduchou rozšiřitelnost pro pokrytí zvyšujících se požadavků na danou síť.

- **Redundance** – nadbytečnost síťových zdrojů v distribuční a páteřní vrstvě zajišťuje celkovou dostupnost celé sítě. Distribuční a páteřní vrstva bývá obvykle připojená více spoji k dalším prvkům sítě. Takže v případě poruchy je síť flexibilní a je schopna rychlého řešení daného problému.

- **Výkon** – vysokorychlostní komunikační linky mezi distribuční a páteřní vrstvou zajišťují dostatečnou šířku pásma pro přenos dat všech koncových prvků v přístupové vrstvě.

- **Jednoduchý management** – každá vrstva vykonává specifické funkce, které můžeme spravovat samostatně a odděleně. Management celé sítě se tím zjednoduší a zpřehlední. V případě poruchy je jednoduché dohledat, kde chyba vznikla a napravit ji.

2.3. Strukturovaná kabeláž

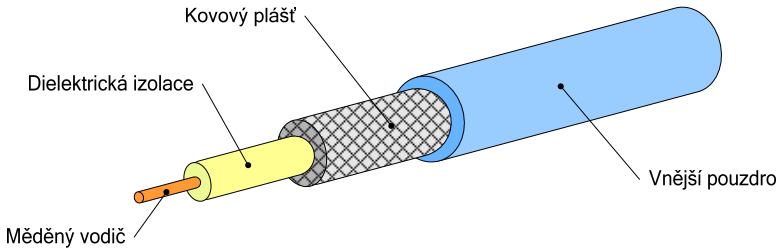
Strukturovaná kabeláž je jedním ze základních prvků infrastruktury lokálních počítačových sítí. V současnosti se kabelový systém využívá nejen pro přenos dat ale také k propojení telefonů nebo pro přenos videosignálu z kamerového systému. [10] Tento trend se zavádí zejména v nově postavených budovách.

Z důvodů dřívější nekompatibility kabelových vedení, byly zavedeny standardy a normy pro budování strukturované kabeláže. Nejpoužívanějším standardem, pomocí něhož jsou budovány kabelážní systémy je standard EIA/TIA 568A. Tento standard definuje systém určený pro komerční a administrativní budovy. Dělí kabelážní systém do tří základních částí a definuje pro ně jednoznačné parametry. Jedná se o pracovní, horizontální a vertikální (páteřní) sekci. Navazujícím standardem na EIA/TIA 568A je standard EIA/TIA 569, který definuje jakým způsobem má být provedena instalace strukturovaného kabelážního systému a to pro jednotlivé sekce zvlášť. [9]

2.3.1. Přenosová média

Pro návrh strukturované kabeláže jsou k dispozici tři základní druhy kabelů. Jedná se o koaxiální kabel, kroucenou dvojlinku a optická vlákna. Koaxiální kabel a kroucená dvojlinka přenáší elektrický signál a jsou založeny na mědi. Optická vlákna nepřenášejí elektrický signál, ale světelný, a jsou tvořena ze skla nebo plastu. V dnešní době se již koaxiálních kabelů nevyužívá, strukturovaná kabeláž je řešena pomocí optických kabelů a kroucených dvojlinek.

Koaxiální kabel (Coaxial cable) – se skládá ze dvou vodičů v pouzdru. Základem je tenký měděný nebo trubkový vodič, který je obklopen nevodivým materiálem a obalen kovem nebo folií sloužící jako zemnění a ochrana proti rušení. Tento kabel je nejstarším médiem pro propojení jednotlivých počítačů. [1] V dnešní době se prakticky už nevyužívá, byl používán pro propojení uzlů ve sběrnicové topologii. Na následujícím obrázku (Obr. 2.2) je zobrazen řez tímto kabelem.

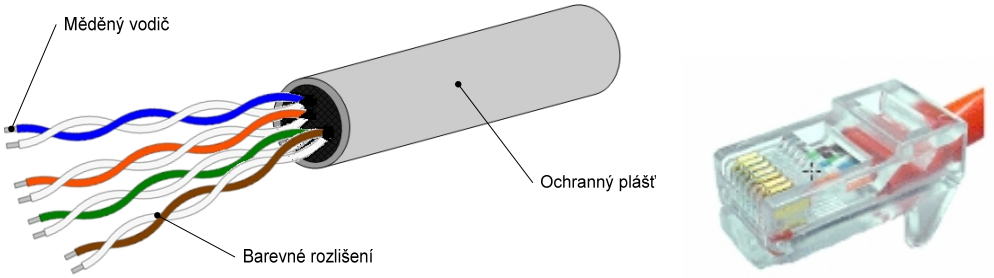


Obr. 2.2: *Koaxiální kabel*

Maximální přenosová rychlost koaxiálních kabelů je 10 Mbit/s a jsou omezeny na maximální vzdálenost mezi uzly 200 až 500 m. K propojení se užívají dva typy konektoru a to N konektor a BNC konektor. Jelikož je tento kabel omezen maximální přenosovou rychlostí, pouze 10 Mbit/s, není prakticky použitelný pro dnešní datové sítě. [1]

Obr. 2.3: *BNC konektor (vpravo) a N konektor (vlevo)*

Kroucená dvojlinka (Twisted Pair) – v současnosti je nejběžnějším a nejpoužívanějším typem kabelu ve výstavbě strukturované kabeláže. Existují dva typy těchto kabelů a to UTP (Unshielded Twisted Pair) nestíněný kabel, který je nejvíce rozšířen u většiny sítí LAN, a STP (Shielded Twisted Pair), který se používá v prostředích náchylných k elektromagnetické interferenci. Kroucená dvojlinka se skládá z osmi samostatně zapouzdřených měděných vodičů, které jsou uspořádány do čtyř párů a každý pár je barevně rozlišen podle standardu T568. Vodiče jsou krouceny v různých úrovních, aby se předešlo vzájemnému rušení. [1] Pro spojení UTP kabelů se používá konektor s označením RJ-45. Na následujícím obrázku (Obr. 2.4) je zobrazen řež kabelem a konektor RJ-45.



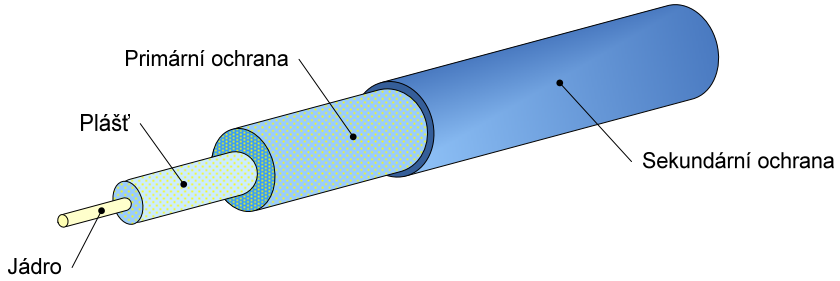
Obr. 2.4: *Kroucená dvojlinka a konektor RJ-45*

Ve strukturované kabeláži rozlišujeme použitou kroucenou dvojlinku na jednotlivé kategorie. Kategorie kabelů nám určují maximální přenosovou kapacitu kabelu a účel použití. Infrastruktura lokálních sítí se řeší výhradně kabely kategorie 5 a výše. Následující tabulka (tab. 2.1) popisuje dostupné kategorie kabelů.

Tab. 2.1: *Kategorie UTP kabelů*

Kategorie	Označení kabelu	Přenosová rychlost [Mbit/s]	Použití
1	Cat 1	1	Telefonní rozvody
2	Cat 2	4	Přenos dat
3	Cat 3	10	Přenos dat 10BaseT
4	Cat 4	16	10BaseT a Token Ring síť
5	Cat 5	100	100BaseT
5e	Cat 5e	1000	100BaseT a ATM
6	Cat 6	1000 a více	1000BaseT
6a	Cat 6a	10000	10GBaseT
7	Cat 7	10000 a více	10GBaseT speciálně stíněný

Optický kabel (Fiber Optic Cable) – optický kabel se zjednodušeně skládá z čirého skleněného nebo plastového jádra, které je obklopeno primární a poté sekundární ochranou. K přenosu dat využívá světelné impulsy (fotony), díky nimž je odolný proti veškerému elektromagnetickému rušení z okolního prostředí. V LAN sítích jsou využívány dva typy optických kabelů – jednovidové (single mode) a multividové (multi mode). [10] Hlavní výhodou optických kabelů je, že mohou přenášet datový signál až na vzdálenosti několika desítek kilometrů a to velmi velkou rychlostí řádově desítky Gbit/s. Na následujícím obrázku (Obr. 2.5) je zobrazen jednoduchý řez optickým kabelem.



Obr. 2.5: *Optický kabel*

V současnosti se optické kabely stále více využívají i v horizontálních rozvodech a nahrazují tak kroucenou dvojlinku. Pro spojení jsou využívány dva typy standardizovaných konektorů – ST (Straight-up) a SC (Straight Conection). Oba typy konektorů jsou zobrazeny na Obr. 2.6.

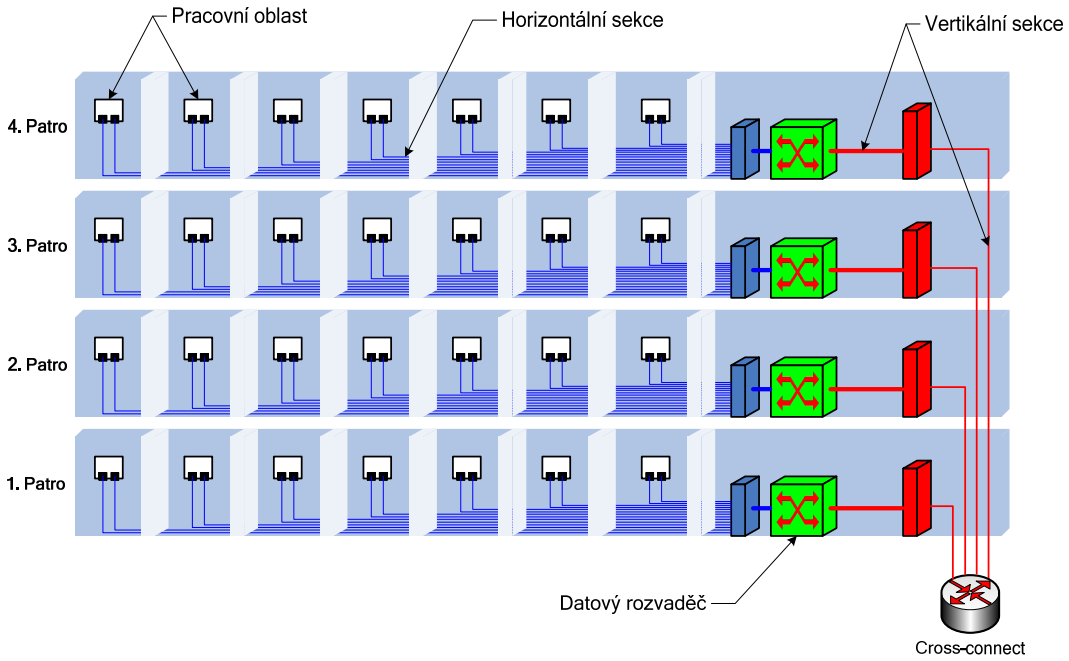
Obr. 2.6: *ST konektor (vlevo) a SC konektor (vpravo) [10]*

2.3.2. Horizontální a vertikální sekce

Při návrhu LAN sítí rozdělujeme strukturovanou kabeláž do tří základních sekcí: pracovní sekce, horizontální sekce a vertikální sekce. Pracovní sekce je částí určitého patra obsluhovanou z jedné telekomunikační místnosti. U UTP kabelů je to oblast do maximální vzdálenosti 50 – 60 metrů.

Horizontální sekce je část kabelážního systému, která propojuje konektory v patch panelech datového rozvaděče s konektory v pracovní oblasti (jednotlivé zásuvky). [9] Tyto rozvody jsou realizovány většinou pomocí metalických kabelů UTP nebo STP, které jsou zakončeny v zásuvkách s konektory RJ-45. Ve výjimečných případech se používají i optická vlákna a to zejména z důvodu překonání větších vzdáleností. Pro horizontální sekci platí omezení, že maximální vzdálenost kabelu od datového rozvaděče nesmí přesáhnout délku 90 metrů.

Dalším, posledním typem kabelážního systému je vertikální sekce (označována také jako páteřní), ta propojuje datové rozvaděče jednotlivých horizontálních sekcí. Rozvody této sekce jsou většinou realizovány pomocí optických kabelů, ale mohou být i metalické. Rozsah vertikální sekce se nemusí vztahovat jen na konkrétní budovu, ale může být i ve více budovách, které jsou od sebe vzdáleny i několik kilometrů. V těchto případech se výhradně používají jen optické kabely. Všechny sekce kabelážního systému jsou názorně zobrazeny na Obr. 2.7.



Obr. 2.7: *Sekce kabelážního systému*

3. SLEDOVÁNÍ A ANALÝZA LAN

3.1. Úvod

V současnosti se počítačové sítě staly nezbytnou a nepostradatelnou součástí všech organizací různých velikostí. S rostoucími požadavky uživatelů a technických pracovníků se stávají stále více rozsáhlejší a komplexnější, často představují složité a rozsáhlé systémy hardwaru a softwaru a vzniklé potíže mají neblahý vliv na produktivitu stovek až tisíců uživatelů. Na provoz reálné sítě má vliv velké množství aspektů, od vlastností pasivních i aktivních prvků, užívané komunikační protokoly, až po samotné síťové aplikace. A proto je nutné, aby správci byli schopni co nejrychleji nalézt nebo lokalizovat příčinu vzniklých problémů a zajistit tak rychlou a efektivní nápravu dané situace. K těmto účelům byly vyvinuty výkonné a všestranné nástroje pro sledování a analýzu provozu v sítích. Analyzátory umožňují krátkodobou nebo dlouhodobou analýzu činnosti sítí a dokáží tak odhalit slabá místa, ve kterých se vyskytují potíže. Bez dat získaných z analyzátorů neexistuje prakticky žádný způsob, jak zjistit, co se v síti děje. Pomocí analyzátorů můžeme například:

- odhalit problémové stanice, u kterých se vyskytují potíže,
- filtrovat a ukládat data na základě různých kritérií,
- identifikovat zdroj a cíl vybraného přenosu dat v síti,
- změřit využití a výkon sítě.

Analyzátory, kromě diagnózy sítě, poskytují pomoc při zhodnocení potřeb pro rozšíření nebo optimalizaci sítě a mohou být použity jako nástroj k umělému zatížení sítě.

3.2. Možnosti sledování a analýzy

Analyzátory můžeme rozdělit do dvou základních skupin a to na softwarové a hardwarové. V případě, že jsou kladeny velké nároky na rychlost a rozsah analýzy, tak se zpravidla využívají hardwarové analyzátory. Pro méně náročné sledování sítě nám postačují analyzátory softwarové. Základní funkce obou skupin analyzátorů jsou stejné. [9]

Prováděné analýzy provozu v počítačových sítích mohou být rozděleny na dva typy. První typ je jednodušší, zahrnuje pouze statistické vyhodnocení různých parametrů provozu (např. zatížení sítě, počet přenesených paketů za určitý čas, apod.). Tento typ analýzy je nenáročný a nevyžaduje velký výkon analyzátoru. Druhý typ analýzy je více komplexnější, vyhodnocují se zde i přenášená data, a proto je náročný na výkon analyzátoru. [9] U tohoto typu se využívají off-line analýzy, tzn. že pakety jsou nejprve zachyceny do vnitřní paměti analyzátoru a posléze podrobeny komplexní analýze.

3.2.1. Softwarové analyzátory

U softwarových analyzátorů zajišťuje veškeré zachytávání, sledování a analýzu softwarová aplikace. K činnosti potřebuje pouze síťovou kartu, která je schopna zachytit všechny pakety procházející síťovým médiem bez ohledu na jejich adresu. Většina dnes vyráběných síťových karet podporuje tuto funkci, která se nazývá smíšený režim (promiscuous mode). Softwarová analýza značně snižuje náklady na analyzátor a může být použita i v méně rozsáhlých sítích. Pro komplexnější analýzy je nutné požít hardwarové analyzátory.

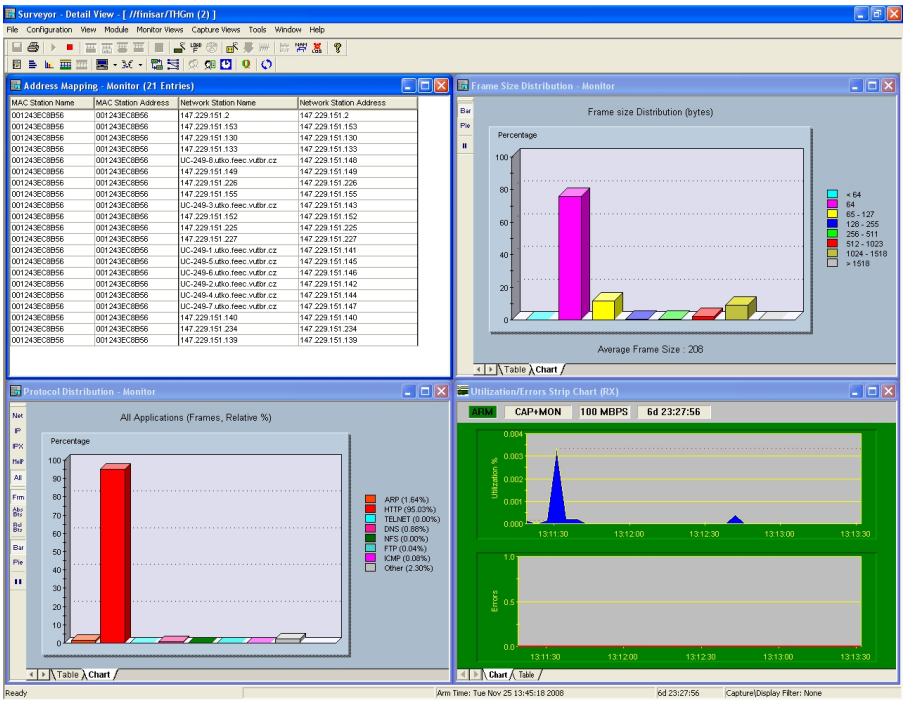
Jeden z nejvýkonnějších komerčních softwarových analyzátorů je v současnosti Observer od známé firmy Network Instruments. Dalším velmi známým softwarem je Surveyor od firmy Finisar Corporation. Kromě profesionálních nástrojů se na trhu objevují analyzátory, které jsou zaměřené na určité oblasti analýzy (např. Wireshark, AiroPeek, WildPacketOmniPeek a mnoho dalších). Jelikož se vyskytuje velké množství těchto analyzátorů, tak jsou v následujícím textu popsány jen některé z nich.

Observer – je rozsáhlý nástroj pro monitorování a sledování sítě, může být použit na systémech Microsoft, Unix, Novell a Apple. Tento analyzátor má velké množství nástrojů a slouží tak k podrobné analýze a diagnostice síťových problémů nebo celé sítě. Umožňuje zachytávání, zobrazení a dekódování síťového provozu v reálném čase, analýzu síťového provozu a diagnostiku kritických problémů, sbírat dlouhodobé statistiky pro zjištění stavu sítě.

Obr. 3.1: *Softwarový analyzátor Observer*

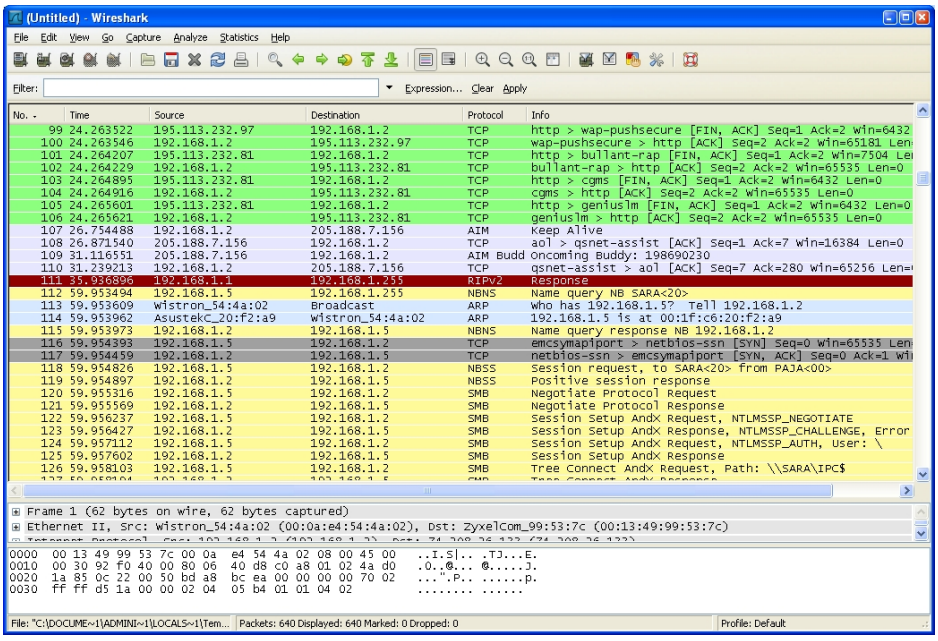
Surveyor – je výkonný, integrovaný nástroj pro monitorování a analýzu 10/100/1000BaseT Ethernet sítí. Pomocí tohoto softwaru jsme schopni provádět více vrstvou expertní analýzu, analýzu sítě v reálném čase, sedmi vrstvé dekódování a analýzu

zachycených dat, filtrování určitého typu paketů a další potřebné analýzy. Surveyor analyzátor poskytuje uživatelům síťovou analýzu a monitorovací nástroj v jednom balíčku.



Obr. 3.2: *Softwarový analyzátor Surveyor*

Wireshark – je nekomerční protokolový softwarový analyzátor, který je schopen zachytit a dekódovat pakety všech známých protokolů. Tento nástroj je vhodný pro zjištění základních informací o datových přenosech v síti.



Obr. 3.3: *Softwarový analyzátor Wireshark*

3.2.2. Hardwarové analyzátory

Hardwarové analyzátory bývají většinou využívány u velkých rozsáhlých sítí, kde není možné získat potřebné statistické a diagnostické informace pomocí běžných softwarových analyzátorů. Obecně jsou hardwarové analyzátory schopny daleko efektivněji a rychleji provádět analýzu a to díky svému připojení (10/100/1000BaseT) přímo do analyzované sítě. Nejsou závislé na pracovní stanici jako softwarové aplikace. Hardwarové analyzátory obsahují speciální okruhy, které slouží k mnohem rychlejšímu a přesnějšímu zachytávání provozu a následné analýze. Většinou jsou kombinovány se softwarovou aplikací, která doplňuje funkce hardwarové části. [1] Toto spojení se označuje jako hybridní analyzátor, hardwarová část implementuje funkce zachytávání a ukládání dat, a softwarová aplikace se pak stará o zpracování, filtrování a zobrazení analyzovaných přenosů.

Hardwarové analyzátory vyrábí velké množství větších společností, které se zabývají IT technologiemi. Nejznámějšími jsou analyzátory od amerických firem Fluke Network a Finisar. Část této diplomové práce se zabývá analýzou LAN sítě pomocí analyzátoru Finisar TGHs od firmy Finisar Corporation. Analyzátor je podrobněji popsán v následující kapitole 3.3.

Fluke Network mimo jiné vyrábí síťový analyzátor pro ethernetové sítě s označením OptiView Link Analyzer (LA), který podporuje analýzu a zachytávání paketů v reálném čase pro plně duplexní Gigabit Ethernet linky. Ve spolupráci se softwarem OptiView Protocol Expert a OptiView console je tento analyzátor velice výkonným nástrojem pro sledování a analýzu rozsáhlé sítě.

Obr. 3.4: *Hardwarový analyzátor OptiView Link Analyzer [5]*

3.3. Síťový analyzátor TGHs

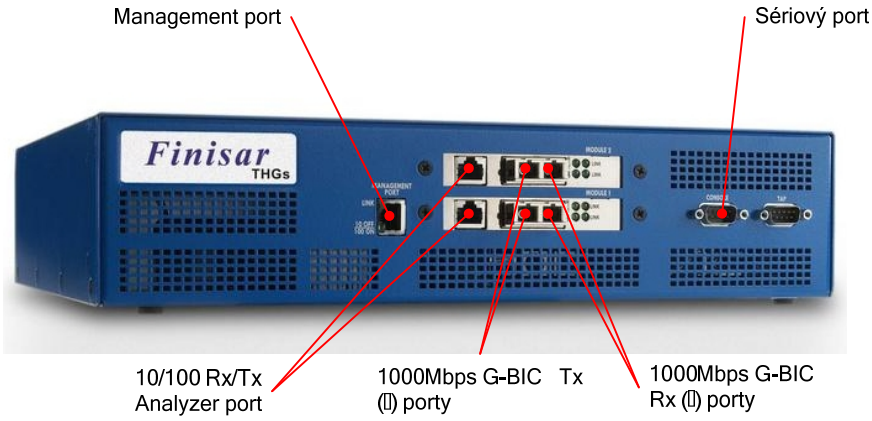
Hardwarový analyzátor Finisar TGHs (dále TGHs) je distribuovaný monitorovací a analytický systém pro rozsáhlé diagnostiky LAN sítí a je přesně navržen pro potřeby IT profesionálů. Může být umístěn přímo v racku data centra nebo strategicky kdekoliv v analyzované síti. Ve spojení se Surveyor software poskytuje nástroje pro účinnou diagnostiku a monitorování plně nebo poloduplexní 10/100/1000 Ethernet sítě v reálném čase. Na následujícím obrázku Obr. 3.5 je zobrazen síťový analyzátor TGHs.

Obr. 3.5: *Hardwarový analyzátor Finisar TGHs [4]*

3.3.1. Popis analyzátoru Finisar TGHs

Jedinečný ASIC (Application Specific Integrated Circuit) design analyzátoru zaručuje, že každý paket (včetně chybných) je zachycen do vyrovnávací paměti přístroje. TGHs je schopný ve spojení se softwarem Surveyor (popsán v kapitole 3.2.1) zároveň provádět monitorování, analýzu a řešení problému v síti a to v reálném čase.

TGHs je vybaven jedním nebo dvěma TGH moduly s 128 MB paměti, podporující různé přenosové rychlosti (10/100Mbps a 1Gbps) pro připojení do segmentu sítě. Může být zapojen jak v poloduplexním režimu (je využit jen jeden modul), tak i v duplexním režimu (jsou využity oba moduly). Analyzátor je také možné připojit k optické síti (1000BaseLx a 1000BaseSx) pomocí SC konektorů. TGHs dále obsahuje dva DB-9 sériové porty, ty slouží k připojení TAP zařízení nebo ke konfiguraci a aktualizaci softwaru. Jednotlivé porty jsou názorně popsány na následujícím obrázku 3.6.



Obr. 3.6: *Popis portů analyzátoru TGHs*

3.3.2. Technická specifikace

V následující tabulce jsou popsány základní technické specifikace analyzátoru Finisar TGHs.

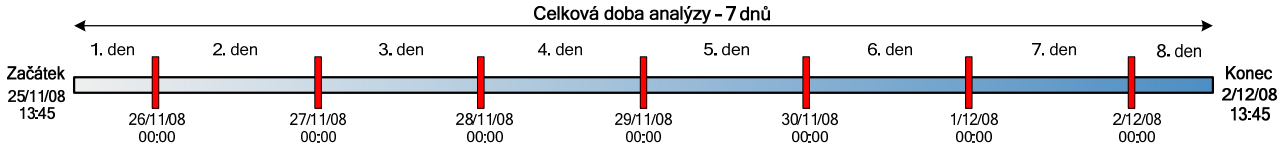
Tab. 3.1: *Technické specifikace Finisar TGHs [4]*

Typ parametru	Parametr		Hodnota
Fyzické parametry	Výška		8,9 cm
	Šířka		37 cm
	Hloubka		35 cm
	Váha		8,2 kg
Pracovní podmínky	Teplota	Pracovní	0° až 40° C
		Skladovací	– 10° až 40° C
	Vlhkost	Pracovní	10 – 95%
		Skladovací	10 – 95%
Napájení	Pracovní napětí		2,5A 250V
	Napájecí napětí		90 – 264 VAC
	Frekvence		48 – 62 Hz
	Spotřeba		160W
	Maximální špičkový proud		40A
	EM kompatibilita		FCC Vlase A, CE
Specifikace portů	Porty k analýze		1000BaseTx – RJ-45 konektor Gigabit Ethernet – Duplex SC konektor (jednovidové nebo mnohovidové) 10/100 Ethernet – RJ-45
	Management port		10/100 Ethernet – RJ-45
	Konzolový port		DB-9 sériový konektor
	TAP port		DB-9 sériový konektor
Provozní specifikace	Přenosová rychlost		10/100/1000 Mb/s
	Velikost bufferu		128MB na modul
	Podporované standardy		10/100/1000BaseT, 1000BaseSx, 1000BaseLx, 1000BaseZx
	Časové rozlišení		25ns

4. ANALÝZA LAN SÍTĚ V LABORATOŘI PA-249 – I

4.1. Úvod

Pro dlouhodobou analýzu byla vybrána LAN síť v laboratoři PA-249. Daná síť se nachází v budově fakulty elektrotechniky a komunikačních technologií na ústavu telekomunikací a byla vybrána s ohledem na rozmanitý síťový provoz. Ke komplexní analýze byl použit hardwarový analyzátor Finisar TGHs od firmy Finisar Corporation (viz. kap. 3.3) ve spojení se softwarem Surveyor verze 6.2. Monitorování vybrané sítě bylo spuštěno nepřetržitě 7 dní (časový průběh monitorování je názorně zobrazen na Obr. 4.1), po tuto dobu analyzátor TGHs společně se softwarovou podporou Surveyor zachytával, monitoroval a analyzoval veškerý provoz a komunikaci ve zmíněné síti. V následující kapitole jsou popsány vybrané výsledky analýzy se zaměřením na použité protokoly.

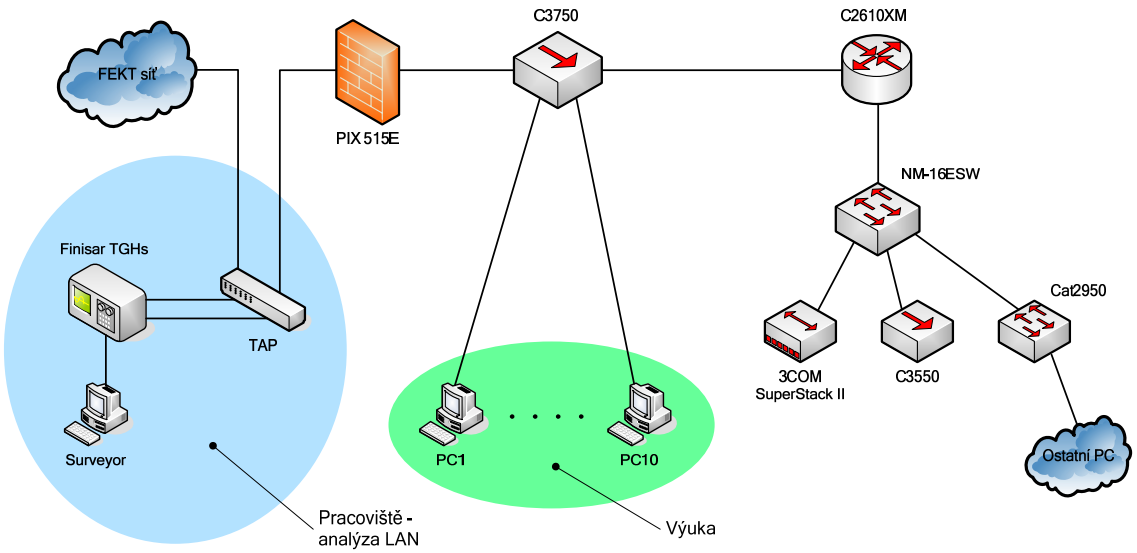


Obr. 4.1: *Časová osa analýzy*

Všechny následující výsledky monitorování jsou vztaženy k této časové ose. Analýza je rozdělena do 8 dnů, ale celkový čas monitorování byl pouze 7 dnů, to je způsobeno začátkem a koncem analýzy (viz. Obr. 4.1).

4.2. Model analyzované sítě

V laboratoři PA-249 probíhá jednak klasická výuka předmětů, tak i praktické části diplomových a bakalářských prací. Schéma monitorované sítě a zapojení analyzátoru je zobrazeno na následujícím obrázku (Obr. 4.2).



Obr. 4.2: *Schéma analyzované sítě*

Síť obsahuje deset pracovních stanic, které jsou určeny pro výuku. Ty jsou připojeny k rozbočovači C3750, a ten následně k firewalu PIX 515E. Celou LAN síť v laboratoři odděluje od fakultní sítě firewal PIX 515E. Směrovač C2610X odděluje ostatní pracovní stanice, které jsou určeny k již zmíněným praktickým částem prací, od sekce pro výuku.

Hardwarový analyzátor byl připojen přes TAP zařízení, v místě mezi firewallem a fakultní sítí. V důsledku toho bylo docíleno, že byl zachytáván veškerý provoz celé LAN sítě v laboratoři. TAP zařízení umožňuje zrcadlení připojených portů, a díky tomu poskytuje hardwarovému analyzátoru prostor pro analýzu v obou směrech aniž by byl narušen běžný provoz. Monitorovaná síť se poté chová jakoby analyzátor nebyl vůbec připojený.

TGHs obsahuje dva moduly pro zachytávání provozu TGHm1 a TGHm2 (viz. kapitola 3.3). Tyto moduly byly připojeny tak, že modul TGHm1 monitoroval provoz ve směru do sítě (Download) a TGHm2 monitoroval provoz ze sítě (Upload). Další důležitou částí analýzy byla pracovní stanice, která byla připojena pomocí síťového kabelu k analyzátoru. Stanice s podporou nainstalovaného softwaru Surveyor zajišťovala sběr, analýzu a zpracování dat zachycených analyzátorem.

4.3. Výsledky dlouhodobé analýzy

Veškeré výsledky analýzy jsou rozděleny do dvou skupin a to na download (data zachycená ve směru do sítě) a upload (data zachycená ve směru ze sítě). Jak již bylo řečeno délka celé analýzy trvala 7 dní, za tuto dobu bylo zachyceno 3 637 171 rámců pro download a 1 585 739 rámců pro upload. V následující tabulce (tab. 4.1) jsou zapsány souhrnné informace o celé analýze.

Tab. 4.1: *Souhrnné informace o analýze*

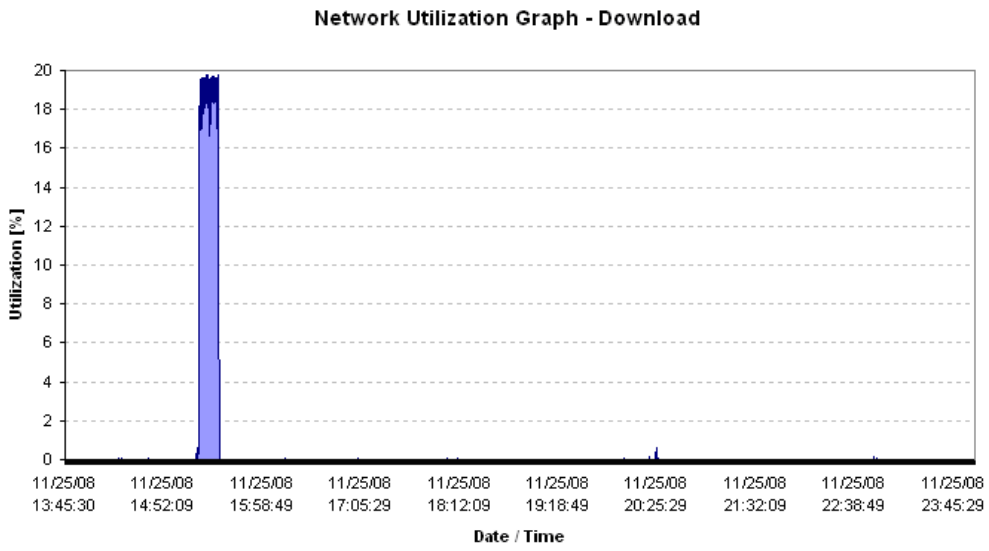
Parametr	Hodnota	
	Download	Upload
Délka analýzy	7d 00h:02m:29s	7d 00h:02m:29s
Zachycené rámce	3 637 171	1 585 739
Broadcast rámce	486 473	45
Multicast rámce	493 493	352
Unicast rámce	2 657 205	1 585 338
Celkový počet přijatých bytů	3 490 411 572	335 188 142
Chybné rámce	0	0
Ztracené pakety	0	0
Počet kolizí	0	0

Analýza byla především zaměřena na nejčastěji se vyskytující síťové protokoly a služby (výsledky jsou popsány v kapitole 4.3). V následující části textu jsou popsány další statistické výsledky analýzy:

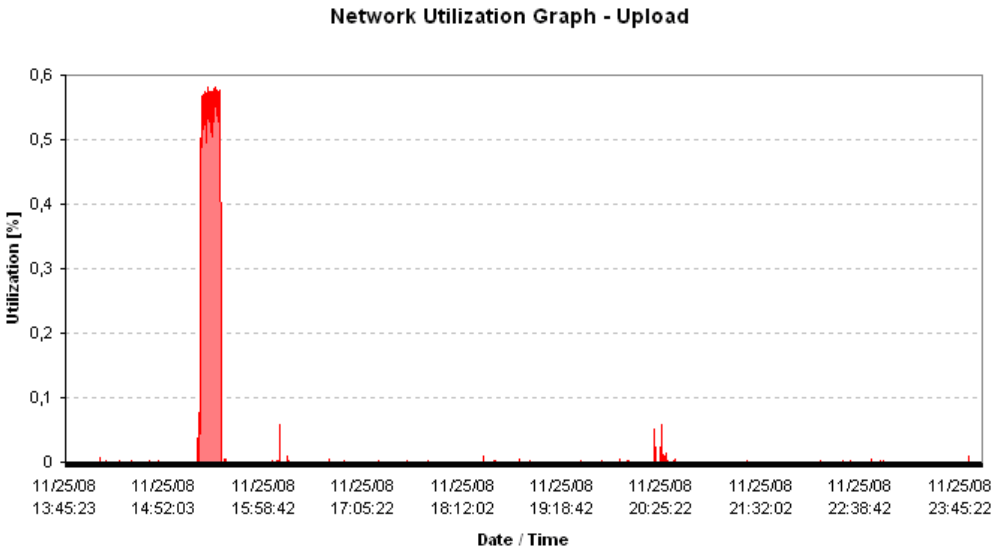
- dílčí a celkové zatížení sítě
- přenos paketů v závislosti na čase
- velikost přenášených rámců

4.3.1. Zatížení sítě

Zatížení sítě je základním a podstatným parametrem všech analýz LAN sítí. Výsledky jsou udávány v závislosti procentuálního zatížení sítě v daném čase, přičemž maximální zatížení odpovídá 100% z kapacity linky (v našem případě 100Mb/s). Na následujících obrázcích (Obr. 4.3 a Obr. 4.4) jsou zobrazeny grafy zatížení linky pro oba směry komunikace v prvním dni analýzy. Další grafy obousměrného zatížení, rozděleny do jednotlivých dnů, jsou zobrazeny v příloze 1.



Obr. 4.3: *Zatížení linky 1. den – download*

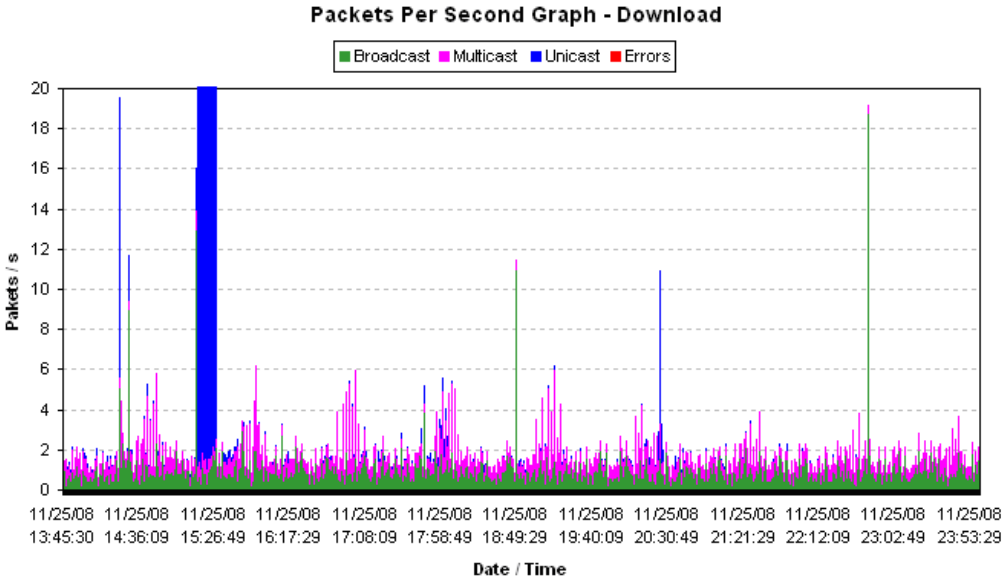


Obr. 4.4: *Zatížení linky 1. den - upload*

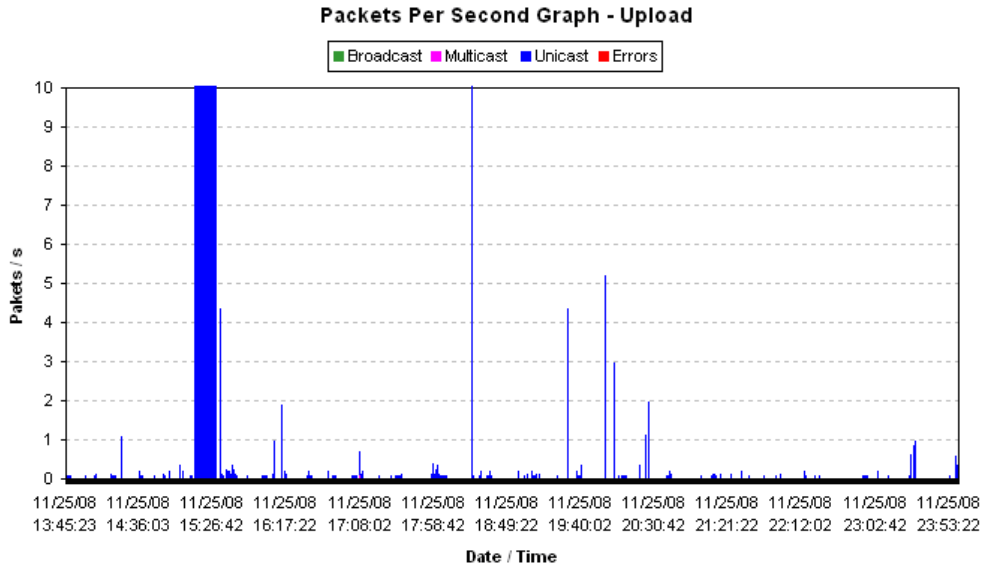
Z výsledků analýzy je patrné, že zatížení sítě v obou směrech bylo velmi malé, v průměru se pohybovalo kolem 2% pro download a 0,1% pro upload. Až na některé případy kdy se zatížení pohybovalo mezi 20% až 70% (download) a 5% až 16% (upload), nebyla síť v průběhu celé analýzy příliš vytížená. Vzniklé špičky jsou pravděpodobně způsobeny větší komunikací v průběhu vyučování v určitých časových úsecích.

4.3.2. Přenos paketů

Dalším analyzovaným parametrem dlouhodobého monitorování LAN sítě byl přenos množství paketů za jednu sekundu a chybovost v závislosti na čase. Tento parametr určuje počet přenesených paketů za jednotku času. Je rozdělen do tří typových skupin, na broadcast pakety, multicast pakety a unicast pakety. Rozhodnutí, zda je paket zařazen do příslušné skupiny, závisí na aplikaci nebo podstatě daného protokolu, kterým je paket přenášen. V analyzované síti nejvíce probíhala komunikace pomocí unicast paketů, jedná se o klasickou komunikaci dvou síťových bodů (klient – server). Na následujícím zobrazení (Obr. 4.5 a Obr. 4.6) jsou grafy závislosti všech typů přenesených paketů a chybovosti pro oba směry síťové komunikace. Jedná se o data naměřená v prvním dni analýzy.



Obr. 4.5: *Množství přenesených paketů a chybovost pro 1. den – download*

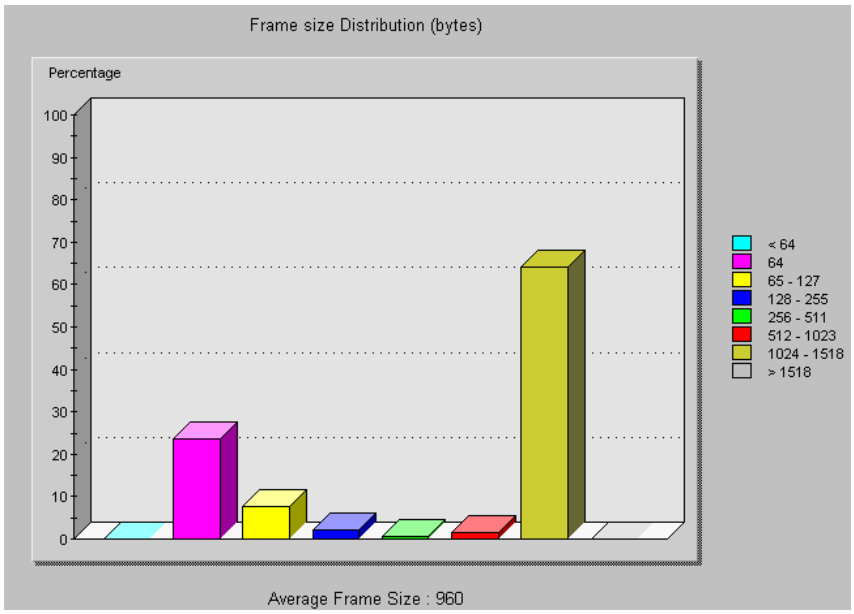


Obr. 4.6: *Množství přenesených paketů a chybovost pro 1. den - upload*

Z naměřených dat je patrné, že celková chybovost v síti byla po dobu celé analýzy nulová. Toto tvrzení také dokazuje tabulka souhrnných statistických údajů provedeného monitorování (tab. 4.1), kde je počet ztracených i chybných rámců roven nule. Přenesené množství unicast paketů je přímo závislé na zatížení v síti, v době vyššího zatížení se analogicky zvýší i počet přenášených paketů. Ve špičkách, které nejsou v grafech zobrazeny z důvodu názorného předvedení dalších typů paketů, dosahovalo množství unicast paketů hodnot 1600 paket/s v download směru a 800 paket/s v upload směru. Četnost přenesených multicast a broadcast paketů byla po dobu monitorování přibližně konstantní, zhruba 2 paket/s a to jen pro směr do sítě.

4.3.3. Velikost přenášených rámců

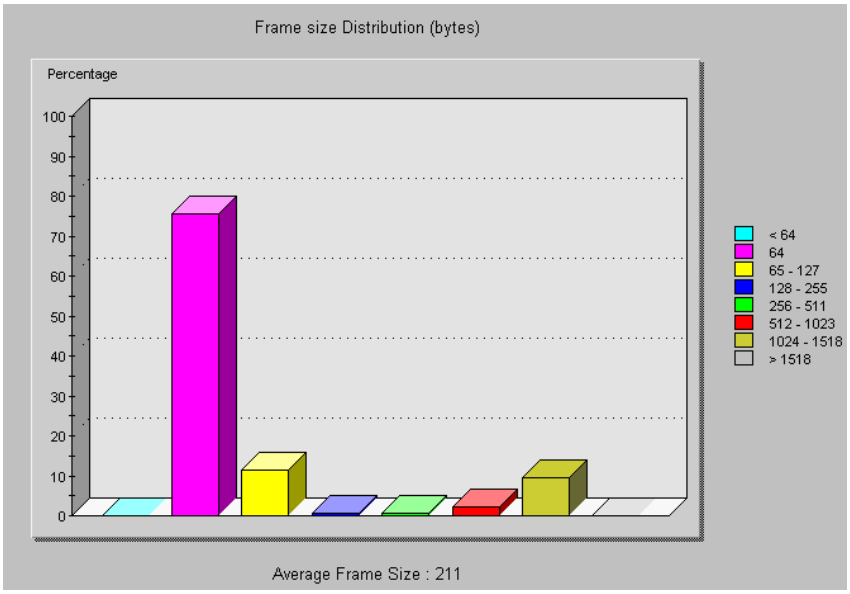
Posledním analyzovaným parametrem byla průměrná velikost přenášených rámců v síti. Je to statistický údaj, který určuje procentuální podíl velikosti jednotlivých přenášených rámců v průběhu celé týdenní analýzy. Parametr je udáván v procentuální závislosti na velikosti rámců v bytech a byl rovněž monitorován jak pro směr ze sítě (upload), tak pro směr do sítě (download). Na následujícím obrázku (Obr. 4.7) je zobrazen graf zmíněné analýzy v download směru.



Obr. 4.7: *Velikost přenášených rámců – download*

Pro download se velikost přenášených rámců v průběhu monitorování pohybovala v rozmezí mezi 1024 – 1518 Byty, tato hodnota odpovídá přibližně 65% všech analyzovaných rámců týdenního monitorování v daném směru. Z velikostí je patrné, že se jedná o ethernet rámce. Druhý největší procentuální podíl (25%) obsadily rámce o velikosti 64 Bytů, jedná se o potvrzovací (ACK) rámce transportního protokolu TCP.

Další obrázek na následující straně (Obr. 4.8) znázorňuje tentýž parametr, ale v opačném směru komunikace (upload).



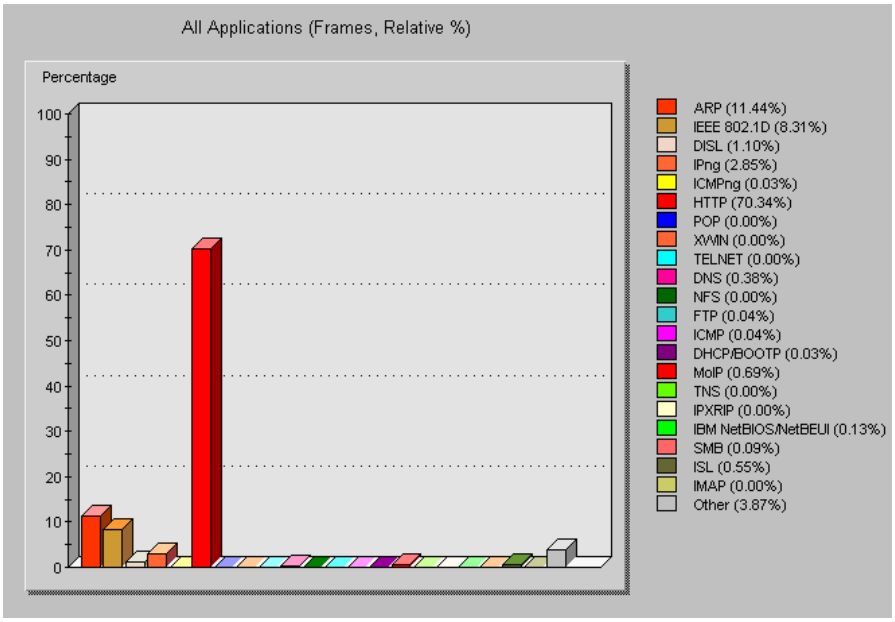
Obr. 4.8: *Velikost přenášených rámců – upload*

V opačném směru (upload) bylo nejvíce přenášených rámců o velikosti 64 Bytů, tato hodnota odpovídá 75% všech přenesených rámců v daném směru. Jedná se tedy opět o potvrzovací (ACK) rámce transportního protokolu TCP. Celková průměrná hodnota velikosti všech přenesených rámců pro download byla 960 Bytů. Pro upload byla tato hodnota rovna 211 Bytům.

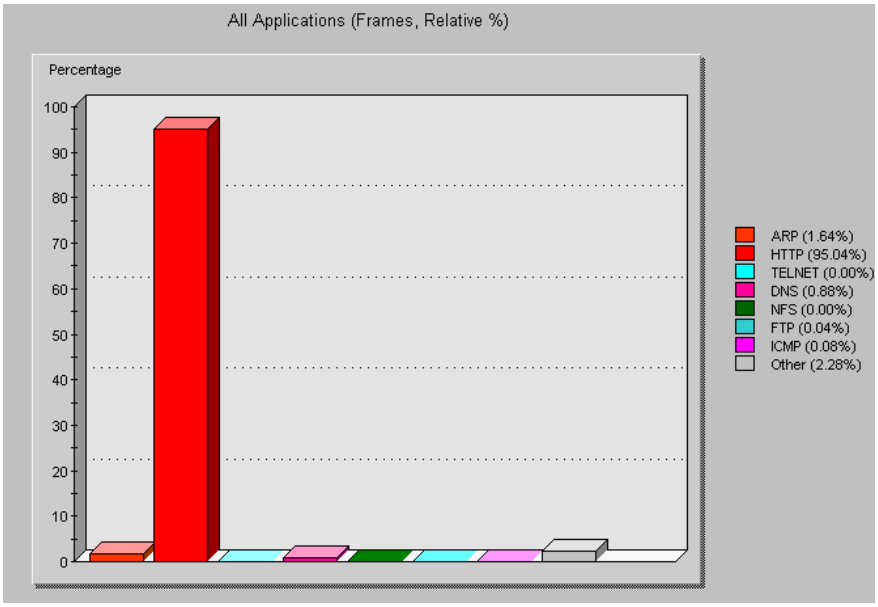
4.4. Výskyt protokolů a služeb

Tato analýza byla zaměřena na nejčastější výskyt protokolů a služeb v síti v průběhu celého monitorování. Tento statistický parametr udává procentuální zastoupení rámců jednotlivých protokolů a služeb, pomocí kterých v analyzované sítí aplikace komunikují.

Výše popsaná analýza byla provedena pro oba směry komunikace v síti a jednotlivé výsledky se od sebe značně liší zejména v počtu zachycených typů rámců. V download směru bylo zachyceno 21 různých služeb na rozdíl od upload směru, kde jich bylo pouze 7. Na následujících obrázcích (Obr. 4.9 a Obr. 4.10) jsou grafy všech protokolů a služeb v obou směrech komunikace.



Obr. 4.9: *Výskyt protokolů a služeb v síti – download*



Obr. 4.10: *Výskyt protokolů a služeb v síti – upload*

Z grafů je patrné, že nejvíce využívanou přenosovou službou v monitorované síti je http služba, která využívá 70,34% veškeré síťové komunikace v download směru a 95,04% v upload směru. Druhým nejvyužívanějším protokolem je arp, který zabírá 11,44% v download a 1,84% v upload směru. V analyzované síti nebyly klasické komunikační služby jako je ftp, telnet, pop, smtp, imap příliš využívány, celkově pokrývají jen 2% přenesených rámců.

Souhrnné shrnutí procentuálního zastoupení všech služeb a protokolů je zapsáno v následující tabulce tab. 4.2.

Tab. 4.2: *Procentuální zastoupení protokolů a služeb v síti*

Protokol / Služba	Procentuální podíl na síťové komunikaci [%]	
	Download	Upload
ARP	11,44	1,64
IEEE 802.1D	8,31	–
DISL	1,10	–
IPng	2,85	–
ICMP	0,04	0,08
HTTP	70,34	95,04
POP	> 0,01	–
XWN	> 0,01	–
TELNET	> 0,01	> 0,01
DNS	0,38	0,88
NSF	> 0,01	> 0,01
FTP	0,04	0,04
DHCP	0,03	–
MoIP	0,69	–
TNS	> 0,01	–
IPXRIP	> 0,01	–
NetBIOS	0,13	–
SMB	0,09	–
ISL	0,55	–
IMAP	> 0,01	–
Ostatní	0,37	2,28

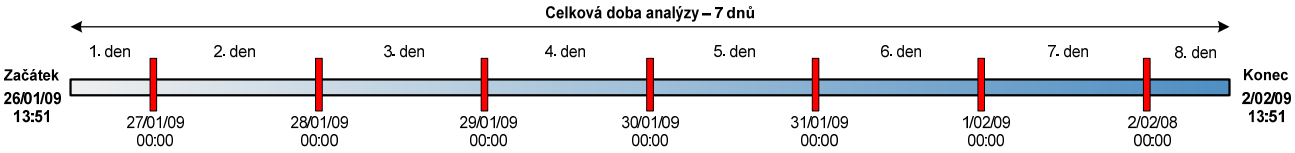
Pod označením „ostatní“ jsou skryty protokoly a služby, které program Surveyor nebyl schopen rozpoznat nebo správně zařadit do příslušné kategorie.

5. ANALÝZA LAN SÍTĚ V LABORATOŘI PA-249 – II

5.1. Úvod

Druhé monitorování LAN sítě v laboratoři PA-249 bylo provedeno pomocí hardwarového analyzátoru Finisar TGHs od firmy Finisar Corporation se softwarovou podporou Surveyor, stejně jako v předchozí analýze. Jedním z mnoha důvodů další komplexní analýzy bylo především malé zatížení LAN sítě a nepatrné využití jednotlivých protokolů a služeb. Předchozí monitorování v podstatě moc nevypovídalo o přenosových schopnostech a možnostech monitorované sítě a tudíž nebyly příliš přínosné k použití v následné simulaci v prostředí OPNET Modeler. Tento nedostatek byl nejvýznačnější příčinou uskutečnění dalšího monitorování LAN sítě s jistými úpravami, které budou v textu dále popsány.

Opětovné monitorování již zmíněné sítě bylo spuštěno nepřetržitě 7 dní, během této doby hardwarový analyzátor společně se softwarem Surveyor monitoroval, zachytával a analyzoval veškerou komunikaci a provoz v síti. Následující obrázek (Obr. 5.1) zobrazuje časový průběh analýzy.

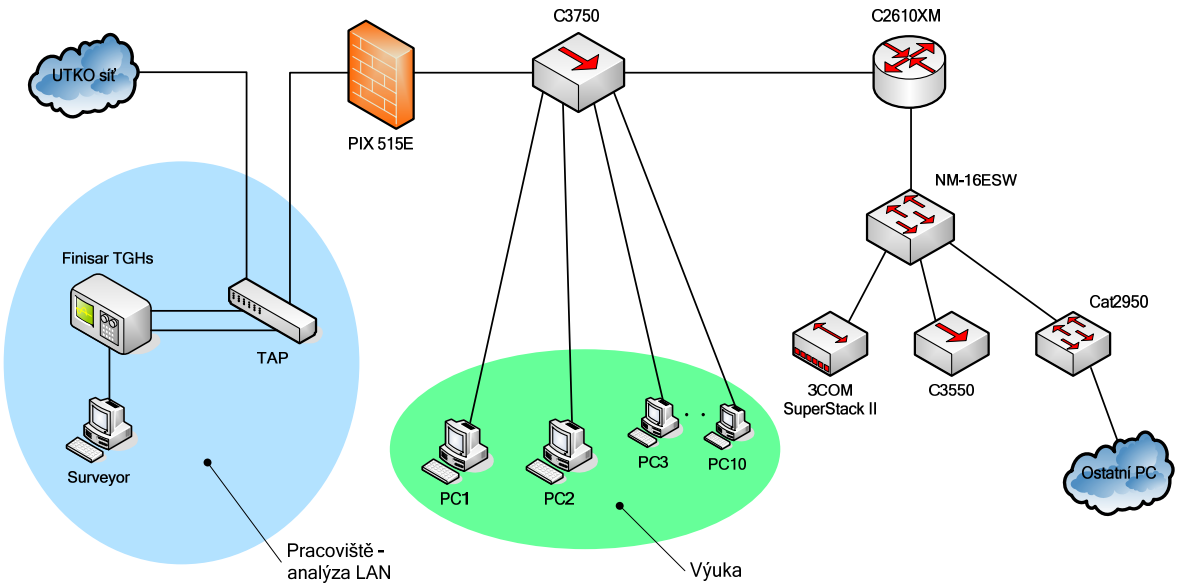


Obr. 5.1: *Časová osa II. analýzy*

V následující kapitole jsou rozebrány a popsány pouze vybrané výsledky, které budou použity jako vstupní data pro simulaci LAN sítě v prostředí OPNET modeler.

5.2. Model analyzované sítě

Druhé monitorování probíhalo v době, kdy se v laboratoři PA-249 nekonala žádná výuka. LAN síť mohla být uměle zatížena a mohly zde být simulovány určité služby, které budou podrobněji popsány v následující části textu. Simulované zatížení bylo zvoleno z toho důvodu, že nebylo možné z předešlé analýzy zjistit specifické chování sítě v určitých stavech, především se jednalo o větší zatížení a nestejnorodý provoz v síti. Schéma monitorované sítě a zapojení hardwarového analyzátoru je zobrazeno na následujícím obrázku (Obr. 5.2).



Obr. 5.2: *Schéma monitorované sítě II*

Zapojení sítě zůstalo totožné jako v předchozí analýze a je podrobně popsáno v předešlé kapitole 4.2. Hlavním rozdílem v tomto monitorování jsou pracovní stanice PC1 a PC2 pomocí nichž byla LAN síť uměle zatěžována. K dosažení simulovaného zatížení sítě byl generován umělý datový přenos s využitím FTP a HTTP služeb. FTP klient na stanici PC1 byl nastaven tak, že opakovaně každou půl hodinu stahoval z FTP serveru, který byl umístěn v jedné z LAN větví ústavu telekomunikací, určitý objem dat. Nastavení FTP klienta na pracovní stanici PC2 bylo velice podobné, pouze s tím rozdílem, že střídavě s FTP klientem na PC1 nahrával v půlhodinových intervalech data na zmíněný server. K přenosu dat pomocí HTTP protokolu bylo využito konstantního streamování videa ze stejného serveru, přičemž příjem byl spuštěn na obou stanicí PC1 i PC2.

Moduly TGHm1 a TGHm2 hardwarového analyzátoru Finisrar TGHs byly k síti připojeny přes TAP zařízení a to tak, že modul TGHm1 monitoroval opět provoz ve směru do sítě (download) a modul TGHm2 provoz ve směru ze sítě (upload). V důsledku tohoto zapojení bylo docíleno plně duplexního režimu monitorování dané LAN sítě aniž by byl narušen běžný chod sítě. K hardwarovému analyzátoru byla dále připojena pracovní stanice s nainstalovaným softwarem Surveyor, která zajišťovala analýzu, sběr a zpracování dat zachycených analyzátorem.

5.3. Výsledky dlouhodobé analýzy

Jak již bylo nastíněno ve čtvrté kapitole, veškeré výsledky dlouhodobého monitorování jsou rozděleny do dvou skupin a to na download (data zachycená ve směru do sítě) a upload (data zachycená ve směru ze sítě).

Celková doba analýzy trvala 7 dní a během této doby bylo zachyceno a analyzováno 327 107 161 rámců pro download a 224 084 768 rámců pro upload, přičemž chybovost v síti byla téměř nulová až na jeden chybný rámec v download směru. Následující tabulka (tab. 5.1) popisuje souhrnné statistické údaje o průběhu celé analýzy.

Tab. 5.1: *Souhrnné informace o analýze*

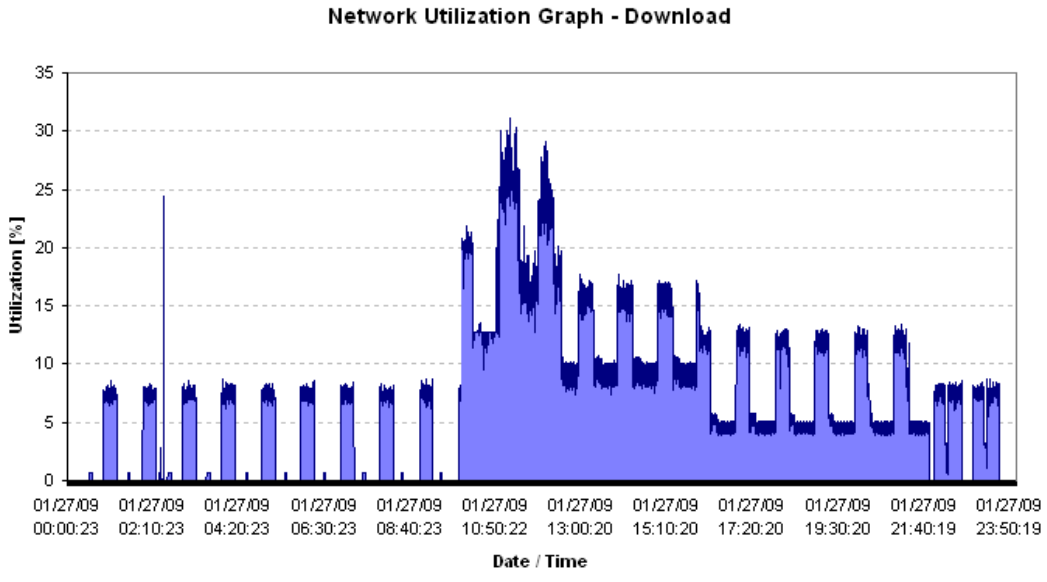
Parametr	Hodnota	
	Download	Upload
Délka analýzy	7d 00h:01m:15s	7d 00h:02m:05s
Zachycené rámce	327 107 161	224 084 768
Broadcast rámce	706 858	0
Multicast rámce	525 927	489
Unicast rámce	325 874 375	224 084 768
Celkový počet přenesených bytů	401 740 188 640	136 518 515 664
Chybné rámce	1	0
Ztracené pakety	0	0
Počet kolizí	1	0

Hlavním cílem této analýzy bylo především získat data potřebná pro simulaci LAN sítě v prostředí OPNET modeler. Následující text proto popisuje jen částečné výsledky dlouhodobého monitorování, které byly použity jako vstup simulace popsané v následující kapitole 6. Monitorování bylo zaměřeno na následující parametry:

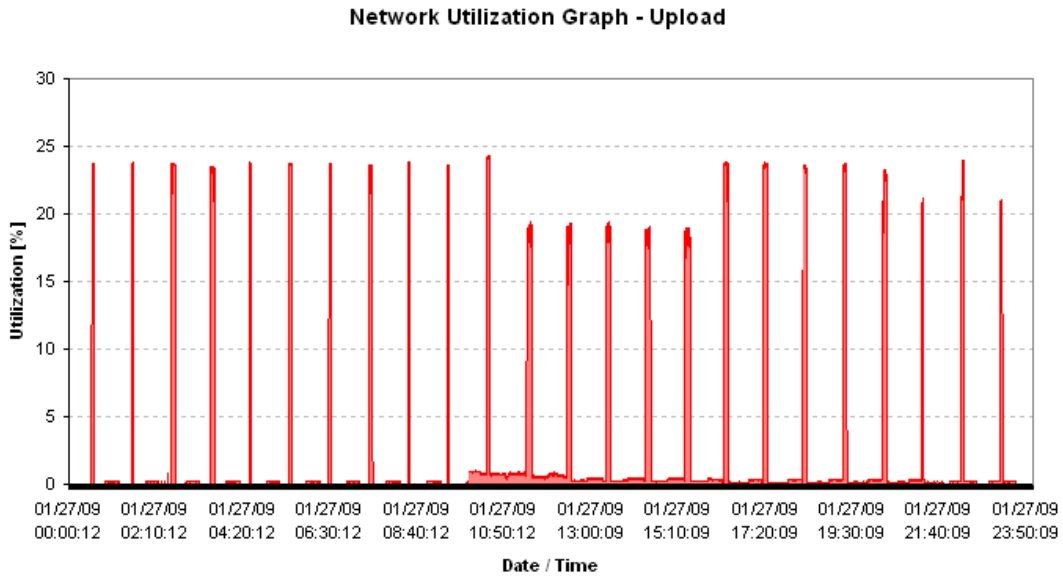
- dílčí a celkové zatížení sítě
- velikost přenášených rámců a chybovost
- výskyt jednotlivých protokolů a služeb

5.3.1. Zatížení sítě

Zatížení je důležitým statistickým parametrem a je udáván v procentuální závislosti na čase, přičemž maximální hodnotě odpovídal datový přenos 100Mb/s. Na následujících obrázcích (obr 5.3 a 5.4) je zobrazeno zatížení pro druhý den monitorování a to pro oba směry síťové komunikace (download i upload).



Obr. 5.3: *Zatížení linky – 2. den II. Monitorování, směr download*



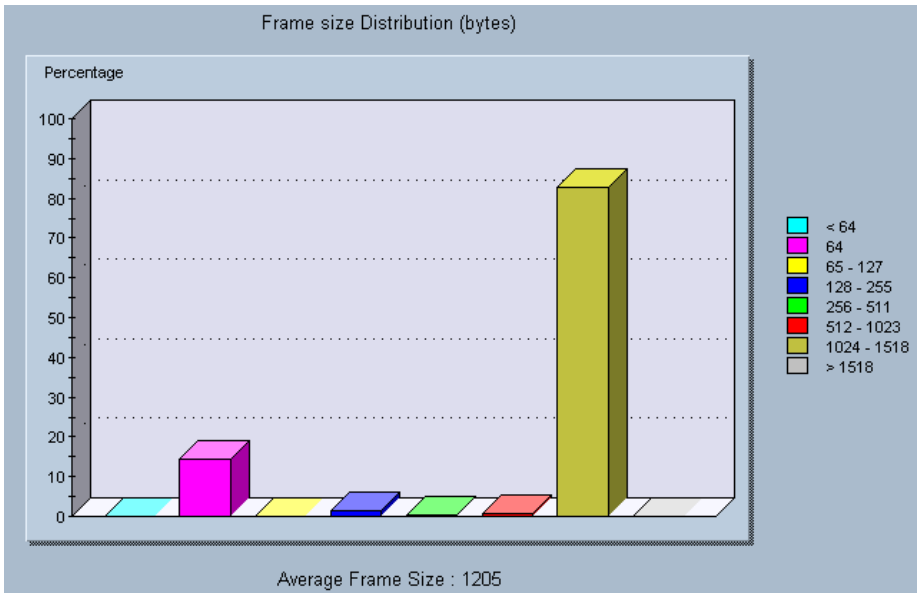
Obr. 5.4: *Zatížení linky - 2. den II. Monitorování, směr upload*

Z naměřených dat je patrné, že pomocí simulovaného datového přenosu na pracovních stanicích PC1 a PC2 (viz. Obr. 5.2) bylo zatížení sítě zvýšeno v průměru na 15% pro download a na 10% pro upload. Ve srovnání s předešlou analýzou LAN sítě, kdy průměrné zatížení v download směru dosahovalo dvou procent a v upload směru pouze desetinu procenta, bylo docíleno podstatně výraznějšího datového přenosu a vytížení kapacity linky. V určitých okamžicích se téměř podařilo síť v download směru zatížit až na její maximální přenosovou kapacitu 100Mb/s. Zatížení v tomto momentě dosahovalo 98%. Nejvyšší zatížení v upload směru bylo přibližně 25%. Další grafy rozděleny do jednotlivých dnů jsou zobrazeny v příloze 3.

5.3.2. Velikost přenášených rámců

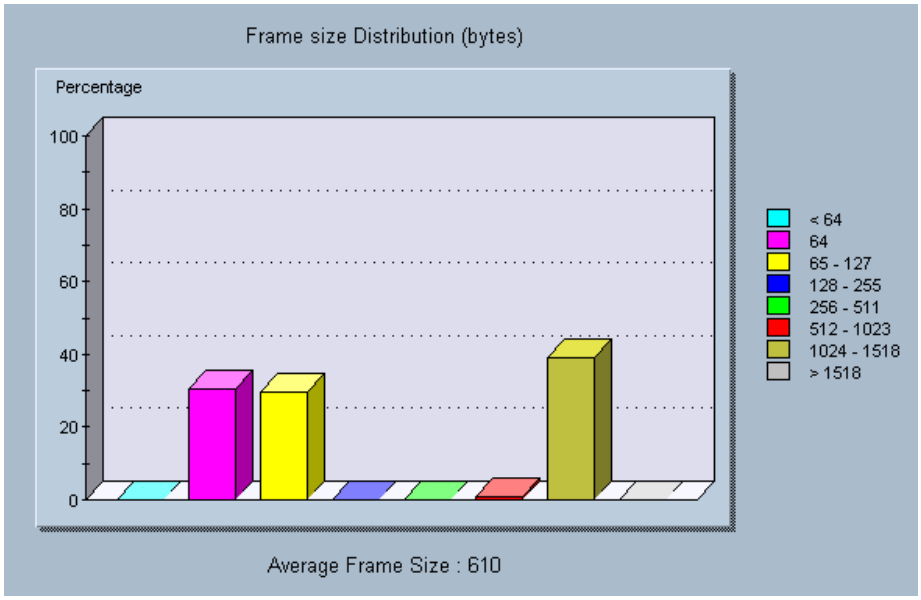
Dalším analyzovaným parametrem byla průměrná velikost přenášených rámců v síti. Tento statistický údaj určuje procentuální podíl velikosti přenášených rámců v průběhu celé týdenní analýzy. Daný parametr byl odděleně sledován pro oba směry síťové komunikace jak pro download, tak i pro upload směr.

Obrázek na následující straně (Obr. 5.5) zobrazuje graf zmíněné analýzy v download směru. V tomto směru se velikost přenášených rámců pohybovala v rozmezí mezi 1024 – 1518 Byty (ethernet rámce), tato hodnota odpovídala 82% všech analyzovaných rámců. Druhé největší procentuální zastoupení (15%) získaly rámce o velikosti 64Bytů, přičemž celková průměrná hodnota velikosti všech přenesených rámců byla 1205 Bytů.



Obr. 5.5: *Velikost přenášených rámců II. monitorování – download*

Na dalším obrázku (Obr. 5.6) je zobrazen tentýž graf, ale v opačném směru síťové komunikace (upload). V upload směru bylo nejvíce přenesených rámců (přibližně 40%) v rozmezí mezi 1024 – 1518 Byty. Druhý největší procentuální podíl (25%) obsadily rámce o velkosti 64 Bytů a rámce o velikosti mezi 65 – 127 Byty. Průměrná hodnota velikosti jednotlivých rámců v upload směru byla 610 Bytů.

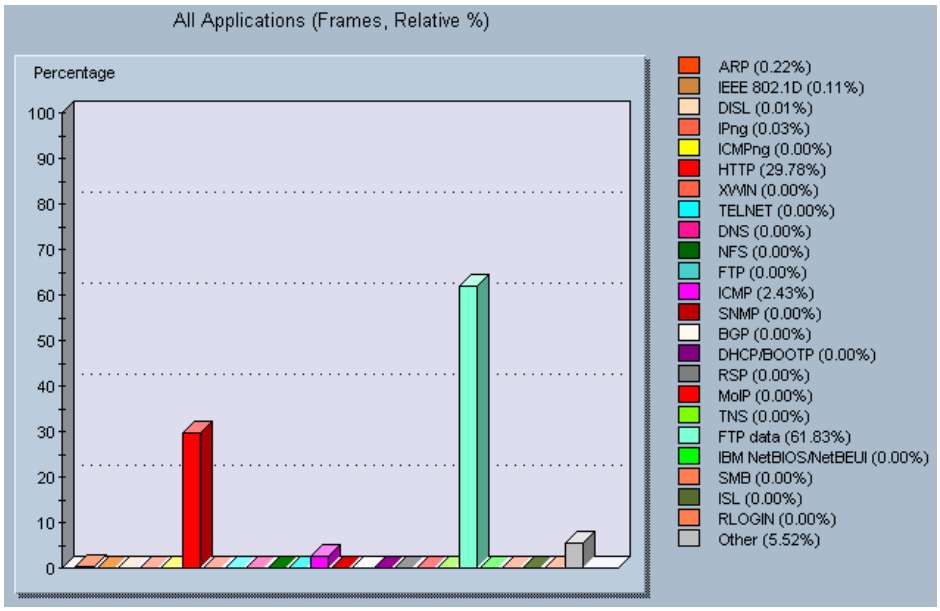


Obr. 5.6: *Velikost přenášených rámců II. Monitorování – upload*

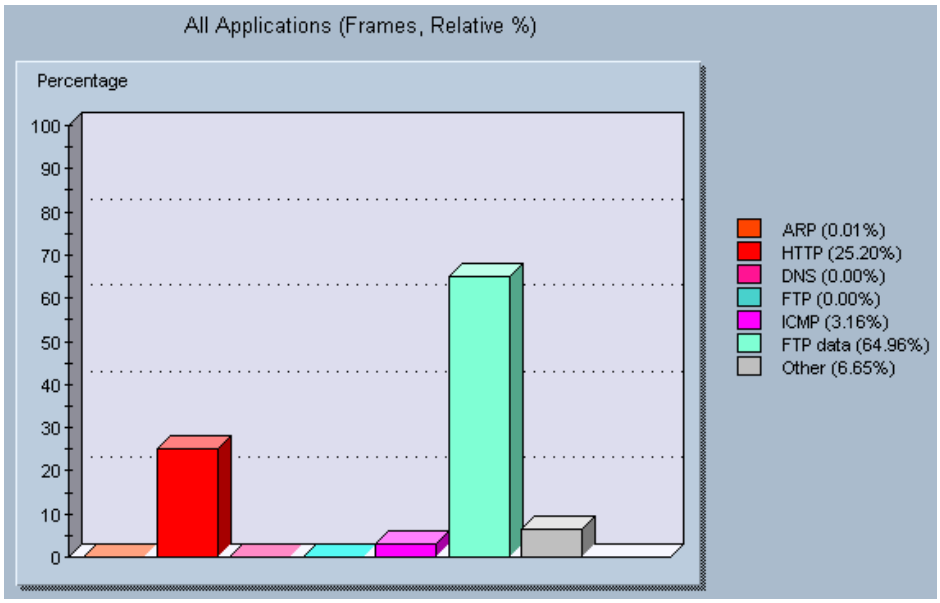
5.3.3. Výskyt protokolů a služeb

Analýza výskytu protokolů a služeb byla provedena pro každý směr síťové komunikace odděleně. Jednotlivé výsledky se od sebe značně liší a to zejména v počtu

zachycených rámců a v procentuálním zastoupení protokolů a služeb. V upload směru bylo monitorováno pouze 7 různých služeb na rozdíl od download směru s 23 službami. Grafy na následujících obrázcích (Obr. 5.7 a obr 5.8) popisují procentuální zastoupení rámců daných protokolů a služeb v průběhu celé týdenní analýzy v obou směrech komunikace.



Obr. 5.7: *Výskyt protokolů a služeb v síti u II. monitorování - download*



Obr. 5.8: *Výskyt protokolů a služeb v síti u II. monitorování – upload*

Z grafů je patrné, že nejvíce využívanou službou v download i upload směru je FTP služba, pomocí které bylo přeneseno více než 61% (download) a 64% (upload) z veškerých rámců zachycených během týdenního monitorování. Druhý nejvíce využívaný protokol byl HTTP protokol. V download směru bylo přeneseno 29% rámců s využitím tohoto protokolu a v opačném směru síťové komunikace 25% ze všech rámců. Zbylé procentuální zastoupení

ostatních protokolů a služeb, které byly v síti po dobu analýzy využívány, je názorně popsáno v následující přehledné tabulce (tab. 5.2).

Tab. 5.2: *Procentuální zastoupení protokolů a služeb v síti – II. monitorování*

Protokol / Služba	Procentuální podíl na síťové komunikaci [%]	
	Download	Upload
ARP	0,22	0,01
IEEE 802.1D	0,11	–
DISL	0,01	–
IPng	0,03	–
ICMPng	> 0,01	–
HTTP	29,78	25,20
XWN	> 0,01	–
TELNET	> 0,01	–
DNS	> 0,01	> 0,01
NFS	> 0,01	–
FTP	> 0,01	> 0,01
ICMP	2,43	3,16
SNMP	> 0,01	–
BGP	> 0,01	–
DHCP	> 0,01	–
RSP	> 0,01	–
MoIP	> 0,01	–
TNS	> 0,01	–
FTP data	61,83	64,96
NetBIOS	> 0,01	–
SMB	> 0,01	–
ISL	> 0,01	–
RLOGIN	> 0,01	–
Ostatní	5,52	6,65

6. SIMULACE LAN SÍTĚ V PROSTŘEDÍ OPNET MODELER

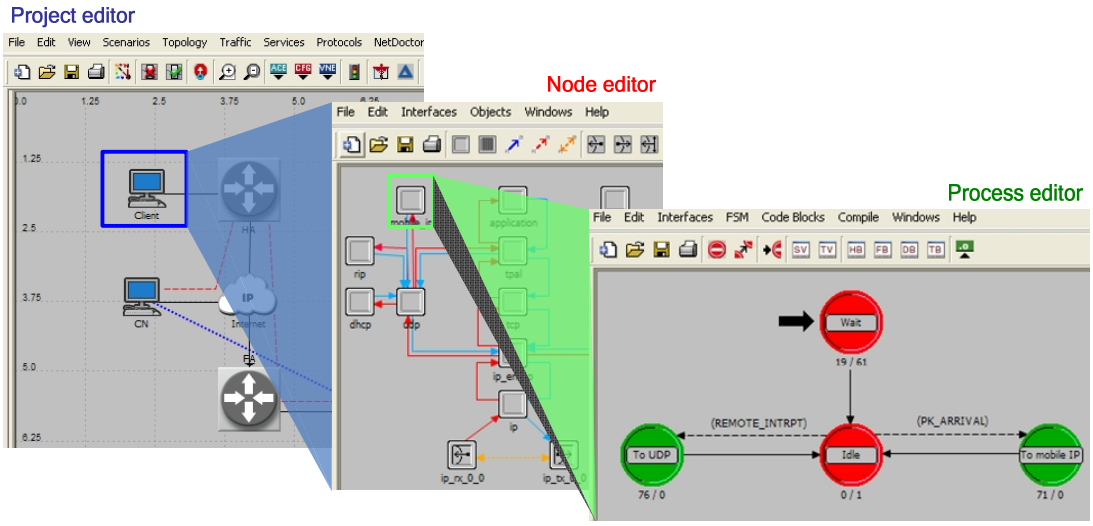
6.1. Úvod

Software OPNET Modeler (dále OM) je moderní simulační nástroj, který byl vyvinut americkou společností OPNET Technologies, Inc. Nabízí širokou škálu využití a to především při návrhu, simulaci a optimalizaci rozsáhlých informačních systémů, jejich protokolů a služeb. [15] Pomocí toho softwaru jsme schopni rychle a efektivně navrhnout a poté nasimulovat chování jakékoliv počítačové sítě ve všech jejich provozních stavech. Hlavní předností OM je možnost monitorování a analyzování širokého spektra nejrůznějších statistik a charakteristik, které jsou uživateli přehledně a názorně předávány v podobě grafických závislostí. Další velkou přínosnou vlastností simulačního prostředí OM je jeho vysoká rychlost zpracování dat během samotné simulace. Je schopen provést simulaci, která by běžně v reálném provozu trvala týdny nebo měsíce, v podstatně kratší době a v to řádově několika minutách nebo hodinách. OM je mocným nástrojem pro firmy zabývající se návrhem a realizací rozsáhlých informačních infrastruktur, umožňuje jim jednoduše a snadno nasimulovat chování budoucí sítě a identifikovat tak potenciální problémy, které by mohly nastat v reálném provozu. Firmy tak mají možnost zdokonalit a optimalizovat případné nedostatky sítě ještě před její vlastní realizací. Další z velkého počtu možností využití OM je při zavádění nových technologií a služeb do již stávajících systémů, a ověřit tak možné dopady na provoz těchto infrastruktur.

Architektura OPNET modeleru je koncipovaná do tří hlavních částí, které jsou na sobě dosti závislé. Jsou jimi:

- project editor – grafický editor topologie sítě,
- node editor – grafický editor funkcí a vlastností uzlu,
- process editor – grafický a textový editor vlastních funkcí jednotlivých procesů.

Následují obrázek (obr 6.1) zobrazuje názorné rozdělení vrstev simulačního prostředí OPNET modeler.



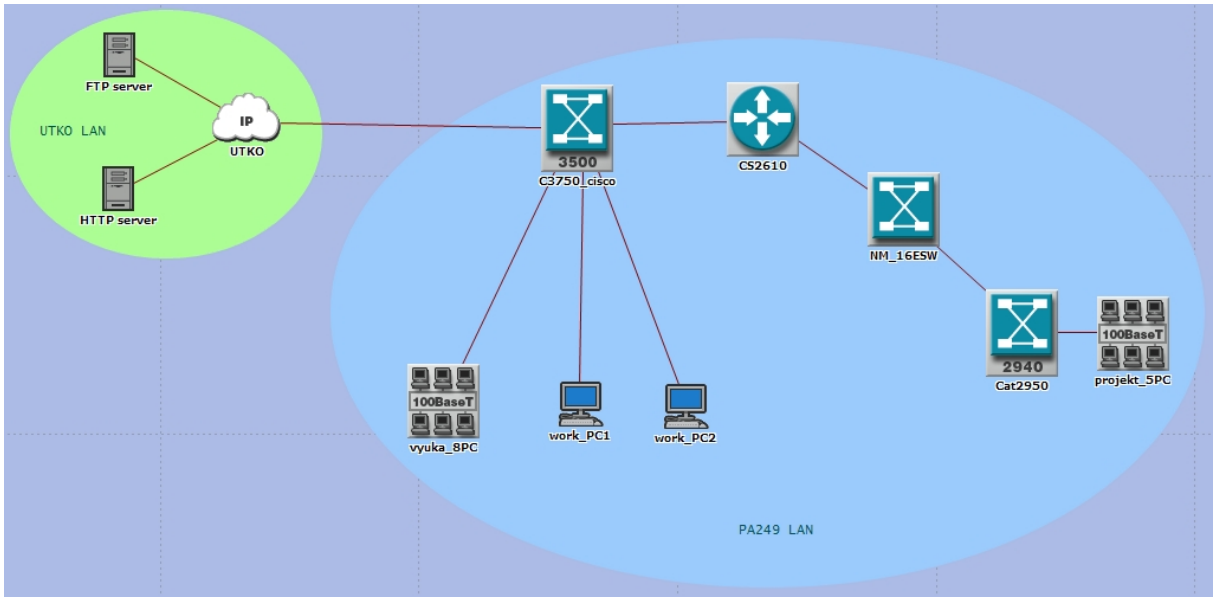
Obr. 6.1: *Architektura OPNET modeler*

6.2. Simulace LAN sítě

Další část práce je zaměřena na simulaci a ověření výsledků analyzované LAN sítě v prostředí OPNET modeler. V tomto prostředí byl vytvořen virtuální model reálné sítě laboratoře PA-249 na ústavu telekomunikací.

6.2.1. Simulační model

Hlavním cílem návrhu a tvorby modelu byla jeho identita a podoba s reálnou LAN sítí v laboratoři PA-249. Proto byly při návrhu zvoleny především reálné modely zařízení od společnosti Cisco Systems, Inc., které OM nabízí ve své základní knihovně. Některé Cisco komponenty, které jsou použity v monitorované síti, knihovna OM nenabízí a proto byly vybrány nejvíce podobná zařízení se stejnými funkcemi a vlastnostmi. Náhrady byly vybrány tak, aby bylo zajištěno největší přiblížení k reálnému modelu. Následují obrázek (Obr. 6.2) zobrazuje simulační model LAN sítě v prostředí OM.



Obr. 6.2: *Model LAN sítě v prostředí OPNET modeler*

Celý simulační model LAN sítě je koncipován jako 100Mbit/s, stejně jako reálný, a vychází ze zapojení monitorované LAN sítě, které je podrobně popsáno v kapitole 4.2. Model obsahuje následující uzlové a koncové prvky:

- přepínače cisco catalyst C3750 a cisco catalyst C2950,
- směrovač CS2610 a přepínač NH16SW,
- 2 pracovní stanice work_PC1 a work_PC2,
- 2 LAN objekty vyuka_8PC a projekt_5PC,
- objekt IP prostředí UTKO a 2 servery zajišťující FTP a HTTP službu.

Jak již bylo zmíněno výše, prvky C3750 a C2950, které jsou použity v reálné síti, byly nahrazeny modely CS3500 a CS2940. Ty neměly žádný vliv na výsledky jednotlivých simulací provozu v síti. Jedná se pouze o různou řadu stejného typu zařízení odlišující se pouze v počtu jednotlivých portů.

Modely LAN sítí vyuka_8PC a projekt_5PC reprezentují skupinu pracovních stanic, které byly k síti připojeny. Tyto modely byly zvoleny pro usnadnění nastavení všech pracovních stanic při pozdějším ověřování schopností a vlastností celé LAN sítě. Objekt vyuka_8PC zastupuje osm běžných pracovních stanic a objekt projekt_5PC jich zastupuje pět. Dále jsou v simulačním modelu (Obr. 6.2) použity dvě speciální koncové pracovní stanice, jedná se o stanice work_PC1 a work_PC2. S využitím těchto stanic byla reálná síť uměle zatěžována, podrobný popis jejich funkce je popsán v kapitole 5.2. Stejně jako v reálné síti, tak i v simulačním modelu zatěžovaly síť a pomocí nich byly ověřeny výsledky dlouhodobého monitorování, které jsou popsány v následující kapitole 6.3.

Dalšími prvky, které jsou použity v simulačním modelu jsou IP prostředí UTKO, FTP server a HTTP server. Společně vytvářejí model jedné z větví LAN sítě na ústavu telekomunikací, se kterou reálná síť během analýzy komunikovala.

6.2.2. Nastavení parametrů simulace

Celková simulace LAN sítě byla rozdělena do dvou částí. První se zabývá ověřením výsledků z dlouhodobého komplexního monitorování, které je popsáno v předešlé kapitole 5. Druhá část je zaměřena zejména na ověření přenosových a kapacitních schopností simulované LAN sítě v reálném prostředí. Nastavení jednotlivých parametrů simulace se pro tyto dvě části v některých bodech nepatrně liší. Rozdíly jsou podrobněji popsány v následujících částech 6. kapitoly (přesněji v bodech 6.3 a 6.4).

Hlavními společnými parametry pro obě části simulací jsou její doba, počet hodnot měřených pro jednotlivé statistiky, automatické přidělování IP adres, verze IP protokolu IPV4. Celková doba simulace byla stejně jako při dlouhodobém monitorování 7 dní. Jednotlivé parametry jsou přehledně popsány v následující tabulce tab. 6.1.

Tab. 6.1: *Společné parametry simulace LAN sítě v OPNET Modeler*

Parametr	Hodnota	Popis
Doba simulace	7 dnů	Udává celkovou dobu při provozu v reálné síti
Počet hodnot	5000	Počet hodnot naměřený pro jednotlivé charakteristiky
Síťový protokol	IP	Udává typ komunikačních adres v síti
Verze IP protokolu	IPv4	Udává verzi použitého IP protokolu

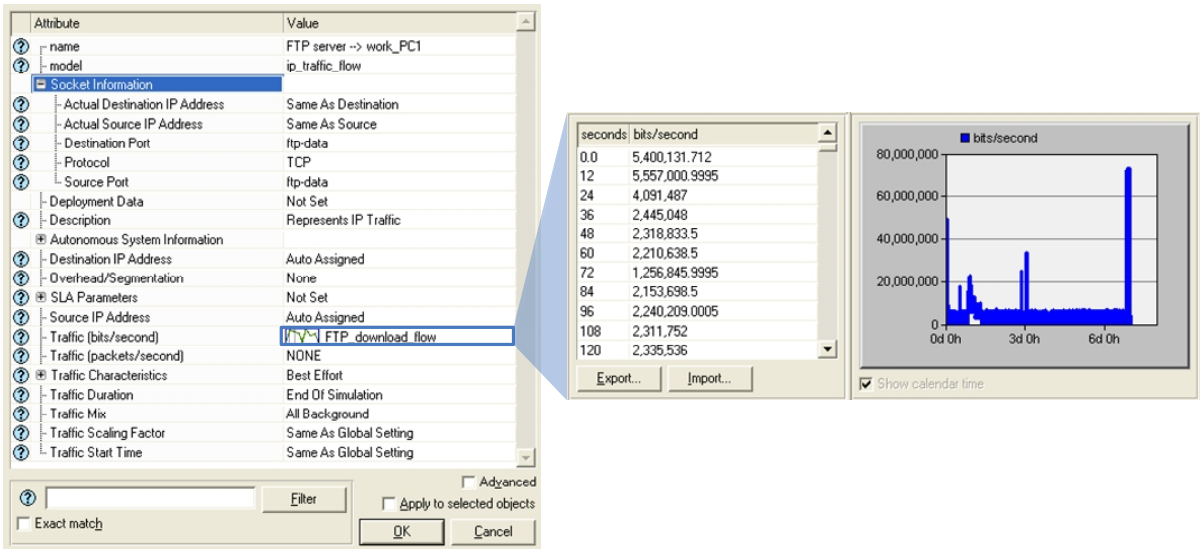
6.3. Ověření výsledků monitorování

Tato část simulace se zabývá chováním simulované sítě při stejných podmínkách a vstupních datech jako v reálné monitorované síti. Cílem ověření výsledků je dosažení stejných přenosových vlastností a parametrů, které byly naměřeny v reálném provozu. Jako vstupní data pro tuto simulaci byla použita naměřená data z dlouhodobého monitorování reálné LAN sítě v laboratoři PA-249 na ústavu telekomunikací.

6.3.1. Import vstupních dat

Vstupní data byla do OM nahrány pomocí textových souborů, které byly vytvořeny programem Surveyor a to z výsledků získaných hardwarovým analyzátorem při dlouhodobém monitorování dané LAN sítě. Především se jednalo o zatížení LAN sítě v obou směrech síťové komunikace.

K importu zmíněných souborů byl použit objekt v OM, který se nazývá ip_traffic_flow. Tento objekt obecně slouží k definovaní IP provozu mezi dvěma uzlovými prvky sítě, dále umožňuje přesně definovat datový a paketový přenos v závislosti na jednotce času. Díky těmto vlastnostem byl zvolen jako nejefektivnější nástroj pro ověření výsledků dat získaných z dlouhodobé analýzy LAN sítě. V simulačním modelu je použit zmíněný objekt ip_traffic_flow mezi pracovními stanicemi (work_PC1, work_PC2), FTP a HTTP servery. Na následujícím obrázku Obr. 6.3 je zobrazena ukázka nastavení objektu ip_traffic_flow včetně importovaných dat, která byla získaná při monitorování.



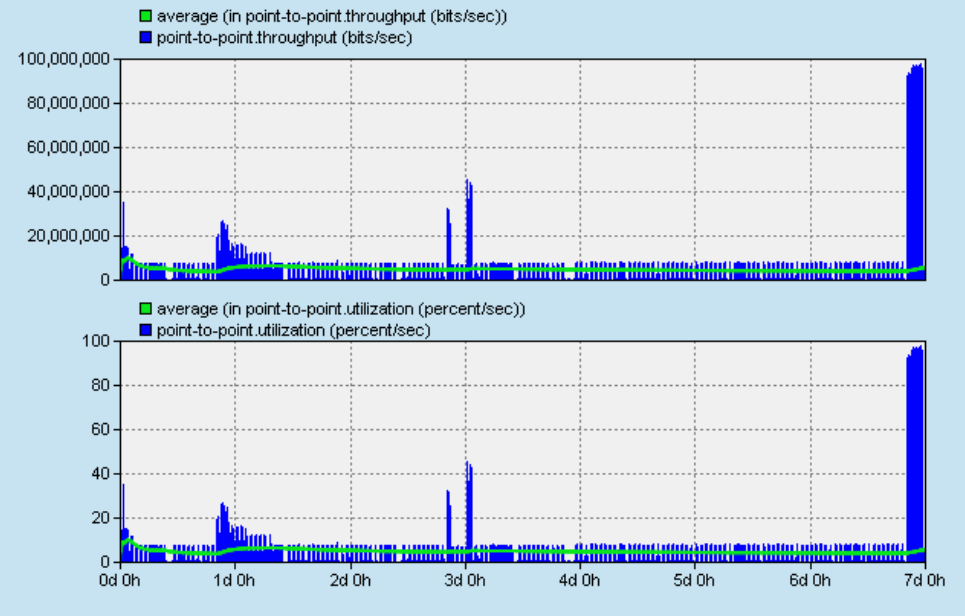
Obr. 6.3: *Nastavení objektu ip_traffic_flow s importovanými daty*

Stejně jako v reálné síti byl datový přenos generován z pracovních stanic work_PC1 a work_PC2 (viz. Obr. 6.2). Množství provozu v download i upload směru bylo mezi stanicemi a servery definováno již zmíněnými importovanými daty, s ohledem na výsledky monitorování využití jednotlivých protokolů a služeb popsané v kapitole 5. Především se jednalo o rozdělení datového přenosu pomocí objektu ip_traffic_flow mezi FTP a HTTP servery. Jelikož se tato část simulace zabývá pouze ověřením výsledku z dlouhodobé analýzy LAN sítě jsou ostatní stanice v síti, stejně jako při monitorování, v podstatě nevyužity a veškerou síťovou komunikaci obstarávají pouze stanice work_PC1 a work_PC2.

6.3.2. Výsledky simulace

Jak již bylo zmíněno, délka simulace modelu LAN sítě byla stejně jako při monitorování 7 dní. Analýza výsledků byla zaměřena na velikost zatížení LAN sítě a na vliv přenosové kapacity na zpoždění ethernet rámců. Veškeré výsledky jsou zobrazeny v podobě grafických závislostí určitého parametru na čase.

Na následujících obrázcích 6.4 a 6.5 je zobrazen datový přenos a zatížení simulované LAN sítě v týdenním horizontu v obou směrech síťové komunikace. Zelená křivka znázorňuje průměrnou hodnotu daného parametru. Z grafů je patrné, že ověření dat získaných z týdenního monitorování reálné LAN sítě proběhlo úspěšně. Simulovaná síť v OM se při stejných podmínkách chová podle předpokladů identicky jako reálná, toto tvrzení dokazují výsledky z dlouhodobého monitorování LAN sítě, které jsou zobrazeny v příloze 3. V porovnání s těmito výsledky je vidět, že velikosti zatížení a datového přenosu jsou přibližně stejné a to v upload i download směru.

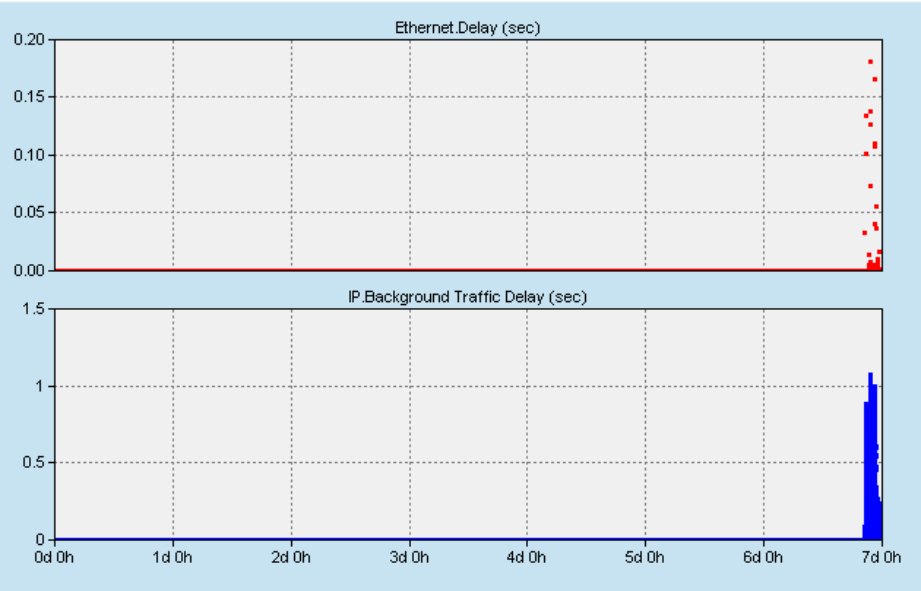


Obr. 6.4: *Datový přenos a zatížení v download směru*

Obr. 6.5: *Datový přenos a zatížení v upload směru*

Pomocí předešlé simulace byla ověřena jedna s funkcí Opnet Modeleru, kdy je možné nasimulovat provoz na základě dat získaných monitorováním reálné sítě.

Na následujícím obrázku 6.6 je zobrazeno zpoždění ethernet rámců a IP paketů v závislosti na čase.



Obr. 6.6: *Zpoždění ethernet rámců a IP paketů*

Zpoždění ethernet rámců a IP paketů nebylo u dlouhodobého monitorování reálné sítě sledováno, ale v simulované síti bylo zajímavé tento parametr monitorovat z důvodů ověření závislosti zpoždění na velikosti zatížení celé sítě. Z naměřených grafických závislostí je vidět, že zpoždění po dobu téměř celé simulace bylo velmi nízké a to méně než 0,01s. Tento stav byl způsoben nízkým zatížením LAN sítě (přibližně do 30%). Při větším zatížení (přibližně 95%) se zpoždění ethernet rámců a IP paketů značně zvýšilo, v našem případě na 0,15s u ethernet rámců a 1,1s u IP paketů. Podstatný rozdíl mezi zpožděním u ethernet rámců a IP paketů byl způsoben tím, že uzly nebyly schopny při vysokém zatížení dostatečně rychle odbavovat pakety v IP vrstvě. Velké zpoždění bylo naměřeno v posledních šesti hodinách simulace.

6.4. Ověření přenosových schopností LAN sítě

Druhá část celkové simulace modelu LAN sítě je zaměřena na ověření přenosových schopností a vlastností dané sítě při určitých simulovaných stavech, které jsou popsány níže v textu. Hlavním cílem této simulace bylo ověřit chování modelu reálné LAN sítě při vysokém zatížení a ověřit tak souhrnné schopnosti vytvořeného modelu. Pro zatížení sítě byl využit uměle generovaný síťový provoz mezi jednotlivými uzly a prvky sítě.

Program OPNET Modeler nabízí funkci, která umožňuje současně simulovat daný model sítě ve více než jedné konfiguraci a poté reportovat výsledky simulací z jednotlivých konfigurací do jednoho společného grafického uspořádání. Tato funkce se nazývá scénář. V naší simulaci bylo celkově vytvořeno 5 různých scénářů simulované LAN sítě. Všech pět simulačních scénářů mělo stejnou hardwarovou konfiguraci a totožné nastavení veškerých

parametrů a vlastností. Odlišovaly se pouze ve velikosti zatížení sítě. Jednotlivá zatížení byla rozdělena podle následujícího schématu:

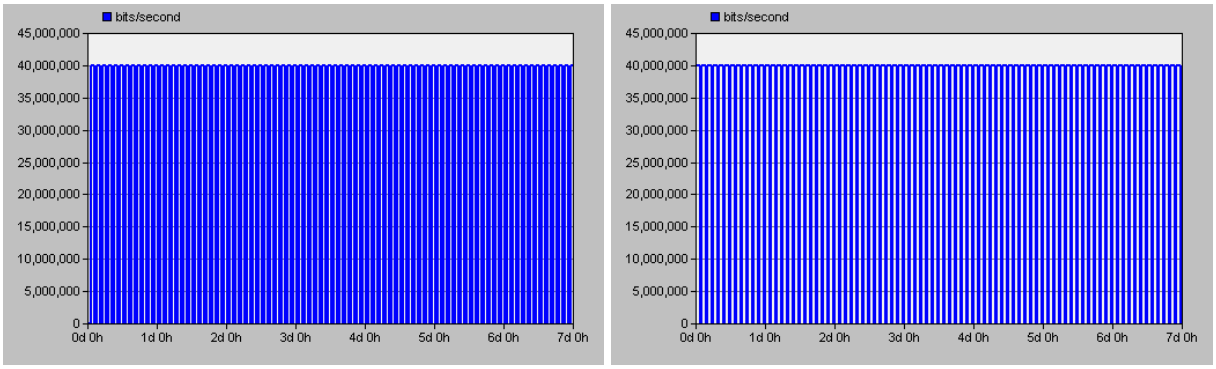
- **1. scénář** – 20 procent zatížení
- **2. scénář** – 40 procent zatížení
- **3. scénář** – 60 procent zatížení
- **4. scénář** – 80 procent zatížení
- **5. scénář** – 98 procent zatížení

Další výsledné grafické závislosti všech simulací budou vždy vztaženy k těmto scénářům a zatížením.

6.4.1. Nastavení zatížení a parametrů simulace

Při umělém zatížení modelu LAN sítě byl opět využit již zmíněný objekt ip_traffic flow (popsaný kapitole 6.3), pomocí objektu byl generován datový přenos ve všech scénářích. K docílení přesně definovaného procentuálního zatížení byl přenos rozdělen do upload a download směru a to tak, aby v součtu bylo dosaženo požadovaného zatížení. Důležitou roli, stejně jako v předchozí simulaci, hrály pracovní stanice work_PC1 a work_PC2 (viz. Obr. 6.2), které byly hlavním zdrojem generovaného provozu.

Jak již bylo zmíněno, uměle generovaný provoz byl rozdělen do obou směrů síťové komunikace a to velmi specifickým způsobem, který zobrazuje následující obrázek (Obr. 6.7).



Obr. 6.7: *Nastavení datového přenosu a) upload, b) download*

Obrázek 6.7 zobrazuje nastavení datového přenosu v objektu ip_traffic_flow pro upload i download směr. V tomto případě se jedná o scénář se zatížením 80 procent celkové přenosové kapacity LAN sítě (100Mbit/s). Jak je vidět na obou obrázcích, maximální hodnota datového přenosu dosahuje pouze k 40Mbit/s. Je to způsobeno tím, že celé zatížení bylo rozděleno mezi oba servery (FTP a HTTP) způsobem v němž půl kapacity směřovalo na FTP server a další část na HTTP server. Zatížení v jednotlivých směrech síťové komunikace bylo definováno tak, že se v hodinových intervalech střídalo stejné zatížení v upload i download směru. Tímto nastavením bylo docíleno, že v součtu bylo celkové zatížení celé LAN sítě na

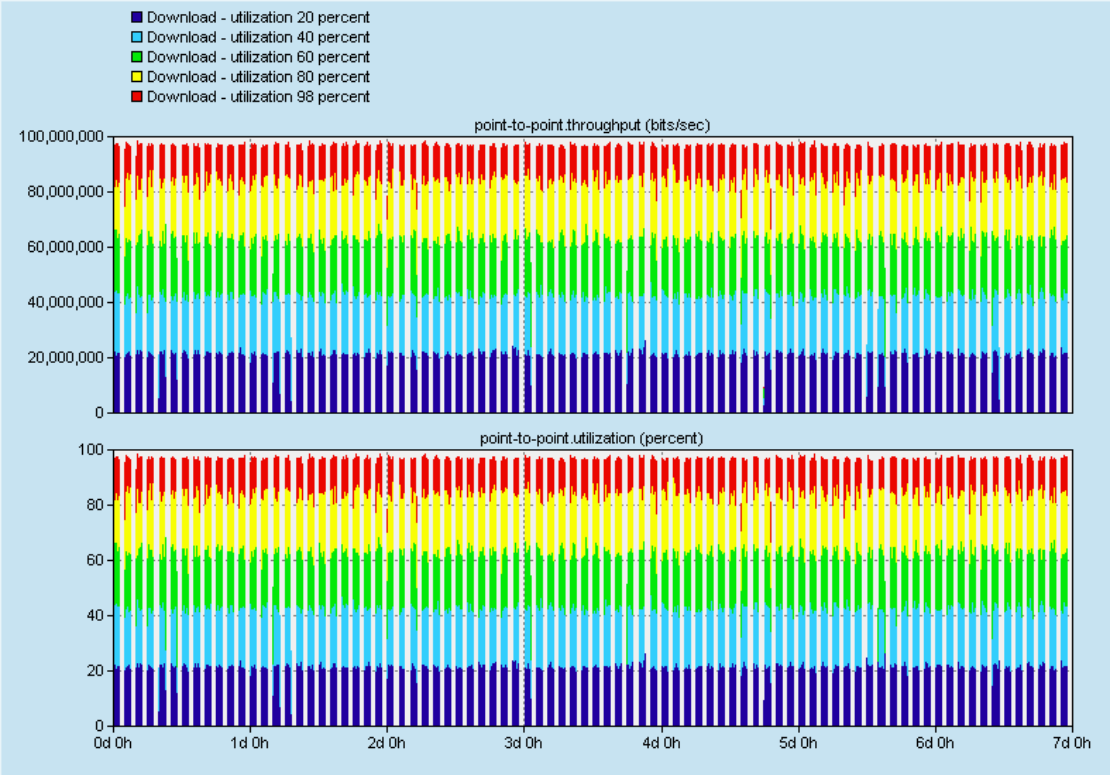
požadované úrovni. Pro ostatní scénáře zůstalo nastavení podobné, jen s rozdílem ve velikosti definovaného zatížení.

V simulované síti byly dále nastaveny aplikace, které provozovaly FTP a HTTP služby. Jednalo se o simulaci klasického provozu v běžných LAN sítích. Konkrétné tyto služby provozovaly všechny pracovní stanice ve skupinách vyuka_8PC a projekt_5PC. Tyto aplikace byly zvoleny z důvodu věrohodnějších výsledků a přiblížení se k provozu v reálných LAN sítích.

Dalším prvkem, který je odlišný od předchozí simulace je nastavení ping příkazu mezi objektem projekt_5PC a IP prostředím UTKO. Tento parametr byl nastaven tak, že opakovaně každou minutu po dobu celé týdenní simulace prováděl ping z objektu projekt_5PC na zmíněný objekt UTKO (viz. obr 6.2). Díky této funkci mohla být sledována závislost odezvy síťového uzlu na velikosti zatížení celé LAN sítě.

6.4.2. Výsledky simulace

Délka celé simulace byla stejně jako v předchozí simulaci zvolena na 7 dní, bylo tak učiněno z důvodů porovnání jednotlivých výsledků z celého monitorování. Analýza výsledků simulace byla zaměřena především na vliv velikosti zatížení celé LAN sítě na zpoždění ethernet rámců, chybovost a odezvu síťových uzlů. Veškeré výsledky jsou zobrazeny v podobě grafických závislostí na čase v porovnání ze všech simulovaných scénářů.



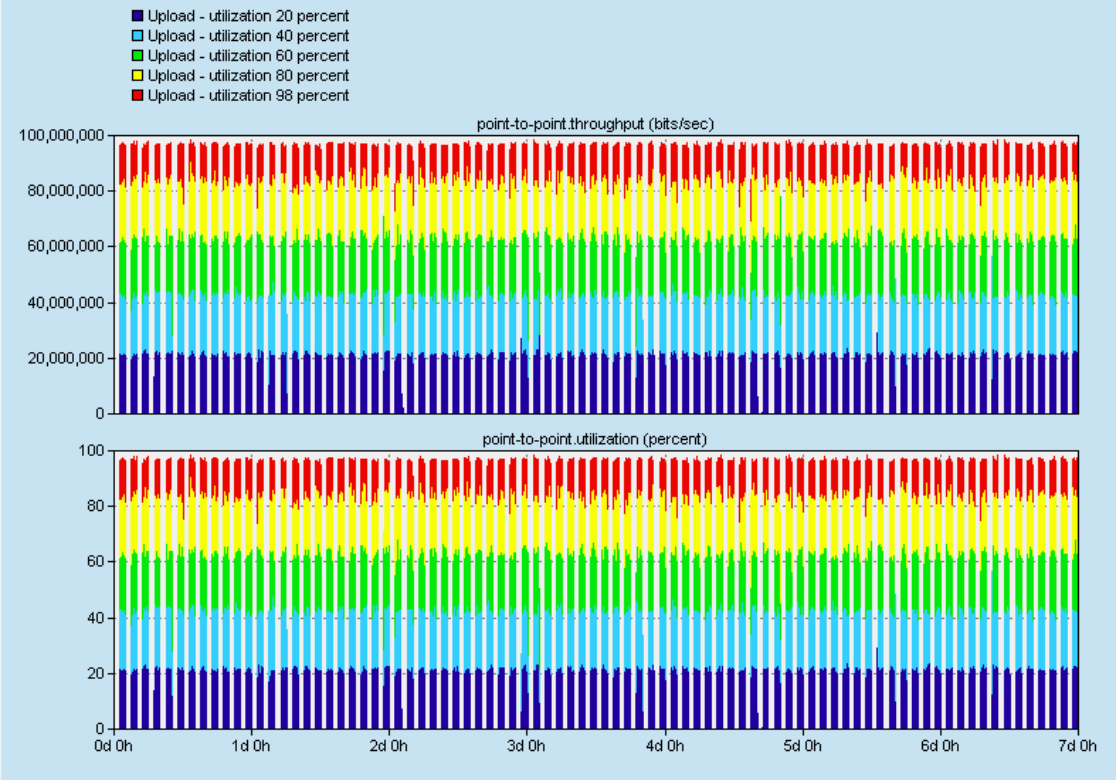
Obr. 6.8: *Datový přenos a zatížení v download směru*

Obrázek (Obr. 6.8) zobrazuje datový přenos a zatížení v průběhu celé simulace. Z grafů na obrázcích 6.8 a 6.9 je vidět, že zatížení v jednotlivých směrech dosahuje

požadované definované hodnoty (20%, 40%, 60%, 80% a 98%). Jak již bylo popsáno v kapitole 6.4, k dosažení celkového zatížení bylo využito toho, že byl definovaný provoz rozdělen v hodinových intervalech střídavě do download a upload směru. Rozdělení je patrné při porovnání obou grafů (Obr. 6.8 a Obr. 6.9).

Pro názornost a porovnání byly veškeré simulace znázorněny v jediném grafickém zobrazení, a jak je naznačeno v legendě grafu, jednotlivé křivky odpovídají danému zatížení v obou směrech síťové komunikace, přičemž každá barevně odlišená křivka odpovídá samostatné simulaci v daném scénáři.

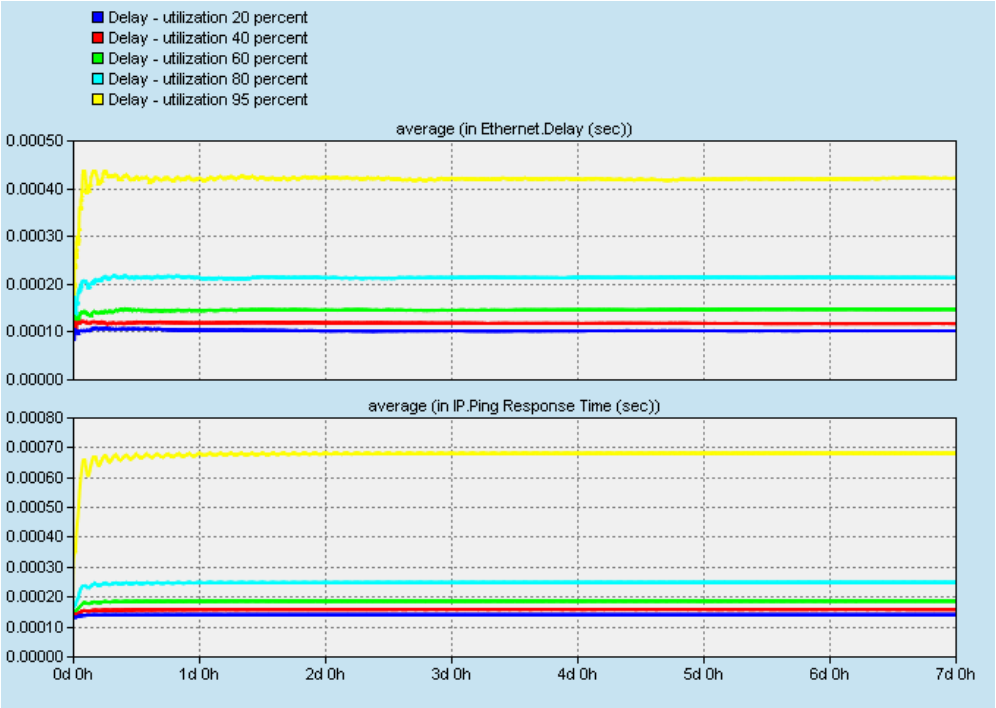
Na následujícím obrázku (Obr. 6.9) jsou zobrazeny stejné parametry, ale v opačném směru síťové komunikace (upload).



Obr. 6.9: *Datový přenos a zatížení v upload směru*

Pro porovnání vlivu velikosti zatížení na zpoždění sítě byly po dobu celé simulace sledovány dva důležité parametry, které se podílí na celkovém zpoždění v LAN síti. Jsou jimi zpoždění ethernet rámců a délka odezvy síťových uzlů.

Obrázek (Obr. 6.10) na následující straně zobrazuje průměrné zpoždění ethernet rámců a průměrnou odezva ping příkazu.



Obr. 6.10: *Zpoždění ethernet rámců a odezva ping příkazu*

Z grafů je vidět, že při zvyšujícím se zatížení celé LAN sítě roste i zpoždění ethernet rámců a odezva ping příkazu. Při zatížení mezi 20 až 80% se zpoždění měnilo jen velmi nepatrně a to od hodnot 0,15ms do 0,25ms pro odezvu ping příkazu a 0,1ms do 0,22ms pro zpoždění ethernet rámců. U zatížení sítě na 98% její celkové provozní kapacity se pomalu začínalo projevovat omezení propustnosti celé simulované sítě. Zpoždění se zvýšilo na 0,43ms u ethernet rámců a na 0,69ms v odezvě ping příkazu. Srovnání vlivu zatížení na propustnost sítě je přehledně zapsáno v následující tabulce tab. 6.2.

Tab. 6.2: *Srovnání vlivu zatížení a propustnosti na průměrném zpoždění LAN sítě*

Scénář	Simulované zatížení [%]	Zpoždění ethernet rámců [ms]	Odezva ping příkazu [ms]
1	20	0,10	0,15
2	40	0,12	0,17
3	60	0,14	0,19
4	80	0,22	0,25
5	98	0,43	0,69

Z nasimulovaných parametrů lze souhrnně zhodnotit, že při zatížení menším než maximální kapacita sítě je zpoždění ethernet rámců a odezva ping příkazu v přijatelných mezích a prakticky nemá větší vliv na schopnost běžného provozu LAN sítě. U aplikací, které byly v síti provozovány (konkrétně FTP a HTTP služba) taktéž nebyly zaznamenány potíže se zvyšujícím se zatížením a velikostí síťového provozu. Celková chybovost a ztrátovost paketů byla po dobu celé simulace nulová.

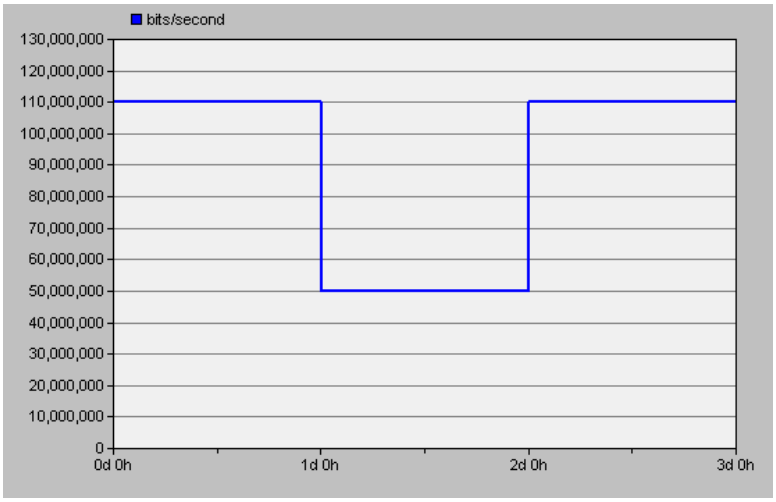
6.5. Teoretické možnosti sítě

Poslední simulace reálného modelu LAN sítě byla zaměřena na ověření teoretického chování sítě při extrémním zatížení. V simulačním modelu bylo ponecháno stejné nastavení veškerých parametrů jako u předchozích simulací. Jediný podstatný rozdíl byl ve velikosti zatížení a v reálné délce provozu celé LAN sítě. Jak již bylo zmíněno, simulace byla zaměřena na specifické chování sítě při určitých podmínkách, a proto byla délka simulace zvolena pouze na tři dny namísto sedmi jako tomu bylo v předchozích simulacích. Tři dny byly postačující na získání potřebných dat k ověření daných parametrů. Hlavním cílem simulace bylo sledování vlivu zatížení na zpoždění ethernet rámců.

K ověření byl použit uměle definovaný síťový provoz se specifickým datovým tokem. Datový tok byl definován následovně (celá síť byla opět koncipována jako 100Mbit/s):

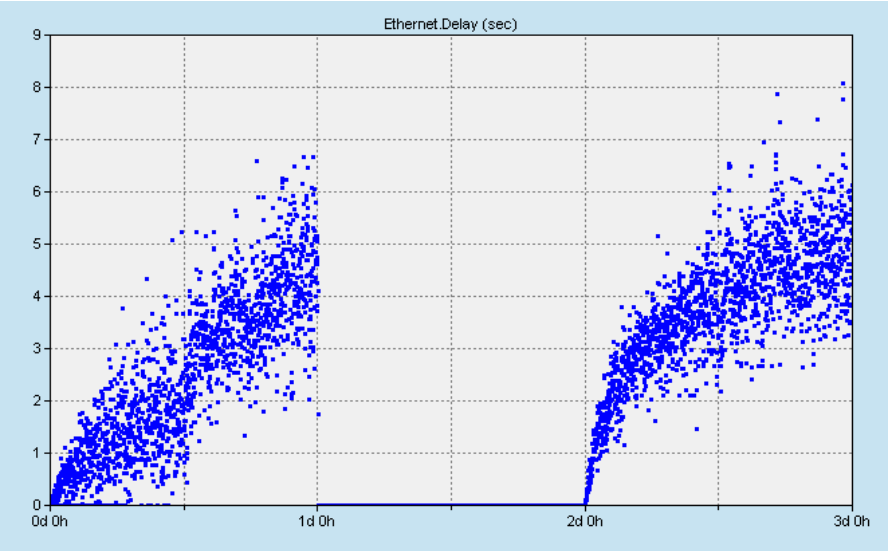
- 1. den byl generovaný datový tok teoreticky 110Mbit/s,
- 2. den 50Mbit/s,
- 3. den byl generovaný datový tok opět teoreticky 110Mbit/s.

Grafické zobrazení zmíněného uměle definovaného IP provozu je zobrazeno na následujícím obrázku (Obr. 6.11).



Obr. 6.11: *Uměle generovaný datový provoz*

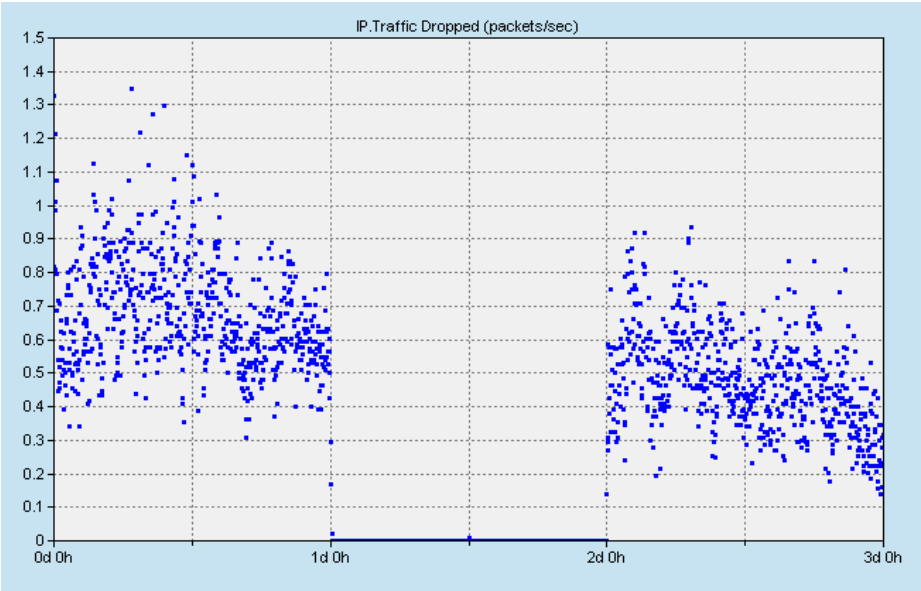
Výsledky simulace jsou zobrazeny na dalším obrázku (Obr. 6.12), jedná se o zpoždění ethernet rámců v závislosti na čase. Výsledky následujícího grafu jsou vztaženy ke grafu na Obr. 6.11, jedná se o stejný časový úsek.



Obr. 6.12: *Zpoždění ethernet rámců*

Z výsledku simulace je patrné, že při zatížení sítě do její maximální kapacity (100Mbit/s) se celá LAN síť chová standardně, zpoždění je minimální a nepřesahuje hodnotu 0,1ms. Jak je vidět v grafu (Obr. 6.12), při tomto zatížení se zpoždění skoro neprojevilo (úsek 1. den až 2. den). Změna nastala až v případě, kdy zatížení sítě vzrostlo na 110Mbit/s. Při tomto zatížení, které bylo o 10% vyšší než maximální přenosová kapacita dané LAN sítě, se zvýšilo rapidně zpoždění ethernet rámců a to exponenciálně až na 6s. V grafu jsou to úseky 0. až 1. den a 2. až 3. den provozu. V podstatě je síť při tomto zatížení nepoužitelná a její provozní vlastnosti jsou velmi malé.

Při tomto teoretickém zatížení se již začíná projevovat vliv ztrátovosti IP paketů. Uzlové prvky začínají zahazovat pakety, které jsou nad rámec přenosové schopnosti dané LAN sítě. Následující obrázek (Obr. 6.13) zobrazuje závislost ztrátovosti paketů na čase.



Obr. 6.13: *Ztrátovost IP paketů*

Z grafu na Obr. 6.13 je vidět, že při teoreticky vyšším zatížení sítě (110Mbit/s) je část dat, která jsou generována nad rámec přenosové kapacity sítě, zahozena a síť je nepřenese. Konkrétně bylo v průměru zahozeno 0,7paketů/s (úseky 0. až 1. den a 2. až 3. den). Úsek 1. až 2. den znázorňuje ztrátovost paketů při zatížení LAN sítě na 50%. Při tomto zatížení se neprojevilo zahazování paketů a celková ztrátovost v tomto úseku je nulová. Celkově lze říci že při standardním zatížení sítě do její maximální přenosové kapacity (100Mbit/s) se ztrátovost (zahazování) paketů neprojevuje, ale v případě zatížení nad rámec přenosové kapacity linky se již ztrátovost paketů začíná uplatňovat.

7. ZÁVĚR

Práce byla zaměřena především na seznámení se a prozkoumání možností sledování a analýzy LAN sítí pomocí hardwarového analyzátoru Finisar TGHs od společnosti Finisar Corporation. Dalším cílem bylo vytvořit model reálné sítě v prostředí Opnet Modeler od organizace Opnet Technologies a za pomoci získaných dat z dlouhodobého monitorování provést simulaci tohoto modelu. Pro dlouhodobou analýzu a monitorování byla vybraná lokální počítačová síť v laboratoři PA-249 na ústavu telekomunikací, jejíž základní model a popis je zobrazen na Obr. 4.2 v kapitole 4.2. Komplexní monitorování a následně pak simulace zmíněné sítě probíhaly po dobu jednoho týdne. Monitorování LAN sítě bylo provedeno dvakrát a to z důvodů, které jsou popsány níže.

První komplexní monitorování LAN sítě (kapitola 4) probíhalo odděleně v obou směrech síťové komunikace a po dobu celé analýzy bylo zachyceno a analyzováno velké množství různých statistických údajů a dat, které jsou v této práci přehledně a názorně uvedeny. Veškeré souhrnné informace o dané analýze jsou popsány v tabulce 4.1. Celá analýza se zabývala zejména základními přenosovými parametry síťové komunikace a nejčastějším výskytem protokolů a služeb v síti. V první části tohoto monitorování jsou popsány výsledky měření celkového zatížení sítě, množství přenesených paketů, chybovosti a průměrné velikosti přenášených rámců. U parametru zatížení sítě bylo sledováno procentuální vytížení sítě v celkovém časovém horizontu. Z výsledků je patrné (Obr. 4.3, Obr. 4.4 a v příloha 1), že zatížení nebylo příliš vysoké, průměrná hodnota byla pouze 2% v download a 0,1% v upload směru a to z celkové přenosové kapacity sítě (100Mbit/s). Dalším podstatným kritériem, které popisuje danou síť, je celková chybovost sítě. V provedeném týdenním monitorování byla souhrnná chybovost v síti nulová. První část monitorování je popsána v kapitole 4.3. Druhá část monitorování je zaměřena na nejčastěji se vyskytující protokoly a služby v průběhu celé týdenní analýzy. Z výsledků, které jsou uvedeny v kapitole 4.4 je zřejmé, že nejčastěji využívanou síťovou službou je HTTP služba, pomocí níž je přenášeno více než 90% veškerých rámců v síti. Zbylé protokoly a služby, které byly po dobu monitorování zachyceny a analyzovány, jsou popsány v tab. 4.2. Tabulka dále poskytuje přehled procentuálního zastoupení všech protokolů a služeb v průběhu celého monitorování. První monitorování LAN sítě i přes získání velkého množství statistických údajů, nebylo přínosné a vhodné pro použití v následné simulaci v prostředí Opnet Modeler. Zejména se jednalo o malé zatížení sítě v obou směrech po dobu celé analýzy. A proto bylo zvoleno další, druhé, monitorování stejné LAN sítě, ale se zaměřením na získání dat potřebných pro následnou simulaci.

Druhé komplexní monitorování LAN sítě (kapitola 5) probíhalo taktéž odděleně v obou směrech po dobu jednoho týdne, od prvního se liší zejména uměle generovaným síťovým provozem, který byl použit po dobu celé analýzy. Umělý provoz byl zvolen z důvodu malého zatížení sítě běžným provozem. Hlavní roli v tomto monitorování představovaly stanice PC1 a PC2 (Obr. 5.2), pomocí nichž byl umělý provoz generován a to velmi specifickým způsobem, který je podrobně popsán v kapitole 5.2. Jak již bylo zmíněno, celá druhá analýza se zabývá především parametry provozu, které jsou následně použity jako vstupní data pro simulaci v Opnet Modeler. Jedná se o dílčí a celkové zatížení sítě, velikost přenášených rámců a výskyt jednotlivých protokolů a služeb. Souhrnné informace týkající se statistických údajů o monitorování jsou popsány v tabulce 5.1. Důležitým parametrem v této analýze byla závislost velikosti zatížení sítě na čase a rozmanitost provozu. Z výsledků dlouhodobého monitorování je zřejmé, že zatížení a rozmanitost provozu byly podstatně vyšší

něž u předchozí analýzy. Z tohoto důvodu byla data získaná z druhého monitorování vhodná jako podklad pro následnou simulaci v prostředí Opnet Modeler. Z výsledků zatížení sítě, které jsou přehledně popsány v kapitole 5.3.1 a v příloze 2, je vidět, že celkové průměrné zatížení sítě v průběhu celého týdenního monitorování bylo 15% pro download a 10% pro upload směr, přičemž maximální přenosová kapacita sítě byla 100Mbit/s. Ve srovnání s předešlou analýzou, kdy průměrné zatížení dosahovalo pouze dvou procent v download a desetinu procenta v upload směru, došlo k podstatnému navýšení datového přenosu a vytížení přenosové linky. Další bližší výsledky druhého monitorování jsou popsány v kapitolách 5.3.2 a 5.3.3.

Další a poslední část práce se zabývá simulací virtuálního modelu reálné monitorované LAN sítě v laboratoři PA-249 a to v simulačním prostředí Opnet Modeler. V tomto prostředí byl vytvořen model LAN sítě, přičemž hlavním cílem návrhu byla jeho podstatná podoba s již zmiňovanou reálnou LAN sítí v laboratoři PA-249. K dosažení co nejvěrnější podoby byly použity reálné modely Cisco zařízení, které Opnet Modeler nabízí ve své knihovně. Přesnější přiblížení použitých prvků je popsáno v kapitole 6.2.

Celková simulace je rozdělena do dvou hlavních částí. První část simulace se zaměřuje na ověření výsledků získaných z druhého monitorování zmíněné LAN sítě. Jako podklad simulace jsou zde použity data získaná z týdenní analýzy, ty byly do prostředí Opnet Modeler nahrány pomocí specifické metody, která je názorně představena v kapitole 6.3. Z výsledných grafů na obrázcích 6.4 a 6.5 lze říci, že ověření proběhlo úspěšně a model LAN sítě se při simulaci v prostření Opnet Modeler chová prakticky téměř identicky jako reálná síť v běžném provozu. Toto tvrzení také dokazují výsledky zobrazené v příloze 2.

Druhá část simulace se zabývá ověřením přenosových schopností a vlastností modelu LAN sítě. Tato simulace je zaměřena na ověření chování modelu při zvyšujícím se zatížení a datovém provozu v síti. Především byl sledován vliv velikosti zatížení celé LAN sítě na zpoždění ethernet rámců, chybovost a odezvu síťových uzlů. K zatížení byl použit uměle generovaný datový provoz a to tím způsobem, že byla síť postupně zatěžována od 20 do 98%. Způsob generování provozu a průběh zatěžování celé sítě je názorně popsán v kapitole 6.5. Z výsledků simulací (Obr. 6.10) s jednotlivým zatížením je patrné, že při zvyšujícím se zatížení roste zpoždění ethernet rámců a odezva síťových uzlů, ale pouze nepatrně a v podstatě toto zpoždění nemá velký vliv na běžný provoz v síti. Výsledky zpoždění jsou přehledně zobrazeny v Tab. 6.2. Celkově lze říci, že při zatížení sítě do 98% její maximální provozní kapacity (100Mbit/s) se síť chová stabilně a podle předpokladů.

Poslední část práce se zaměřuje na ověření chování sítě při teoretickém zatížení, které je vyšší než její maximální přenosová kapacita. Při simulaci byla celá LAN síť zatížena o 10% vyšším datovým tokem než je maximální datový tok v síti (100Mbit/s). Z výsledků simulací bylo zjištěno, že při tomto zatížení síť vykazuje rapidní navýšení zpoždění ethernet rámců, v průměru na 3s, a celkově se celá síť stává nepoužitelnou pro běžný provoz. Při tomto zatížení se již začíná projevovat ztrátovost paketů, síť část dat, která jsou nad rámec její přenosové kapacity nepřenese. Vývoj zpoždění ethernet rámců a zahazování IP paketů lze názorně vidět na grafickém zobrazení (Obr. 6.12 a Obr. 6.13), kde jsou zachyceny výsledky při běžném a teoretickém zatížení.

8. SEZNAM LITERATURY A POUŽITÝCH ZDROJŮ

[1] BIGELOW, J. S. *Mistrovství v počítačových sítích, správa, konfigurace, diagnostika a řešení problémů*. Computer Press, Brno, 2004.

[2] DOSEDLA, M. *Technologie počítačových sítí* [online]. 2006 [cit. 2008-11-21]. URL: <http://www.ped.muni.cz/wtech/elearning/teps.pdf>

[3] DOSTÁLEK, L., KABELOVÁ, A. *Velký průvodce protokoly TCP/IP a sytému DNS*. Computer Press, Praha 2000.

[4] FINISAR CORPORATION, *THGs and THGsE Distributed Monitoring and Analysis Systém – User's Guide* [online]. 2004 [cit. 2008-12-02]. URL: <http://www.finisar.com/product-295-THG_Surveyor_Ethernet_Analyzer>

[5] FLUKE NETWORK CORPORATION, *OptiView Link Analyzer – Data sheet* [online]. 2006 [cit. 2008-12-02]. URL: <http://www.flukenetworks.com/>

[6] OLIFER, N., OLIFER, V. Computer *Networks: Principles, Technologies and Protocols for Network Design*. Chichester: John Wiley & Sons, 2006.

[7] JANEČEK J., BÍLÍ M. *Lokální sítě*. Skriptum ČVUT FEL, Praha 2003.

[8] MACHAR T., *Síťový protokol TCP/IP* [online]. 2004 [cit. 2008-11-22]. URL: <http://www.maturita.cz/referaty/informatika/tcp_ip.htm>

[9] MOLNÁR K., SOUMAR M., *Praktikum z informačních sítí*. Skriptum VUT FEKT, Brno 2002.

[10] ODVÁRKA P*., Strukturované kabeláže* [online]. 2001 [cit. 2008-12-02]. URL: <http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&temaID=48&clanekID=61>

[11] ODVÁRKA P., *Základy topologie a komunikace* [online]. 2000 [cit. 2008-11-22]. URL: <http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&temaID=1&clanekID=21>

[12] PETERKA J., *Archív článků a přednášek* [online]. 2006 [cit. 2008-11-8]. URL: <http://www.earchiv.cz>

[13] ŠKORPIL V., GREGOŘICA M. *Vysokorychlostní komunikační systémy*. Skriptum VUT FEKT, Brno 2003.

[14] WIKIPEDIE otevřená encyklopedie, *IP datagram* [online]. 2008 [cit. 2008-11-22]. URL: <http://cs.wikipedia.org/wiki/IP_datagram>

[15] SKOPAL J., *Optimalizace provozu vysokorychlostní sítě,* Bakalářská práce, VUT FEKT, Brno 2007.

[16] OPNET TECHNOLOGIES, *Opnet Modeler Produkt - Documentation Release 14.5*, Opnet Technologies Inc., 2008.

[17] McCABE, J.: *Network Analysis, Architecture, and Design*. San Francisco: Morgan Kaufmann, 2007.

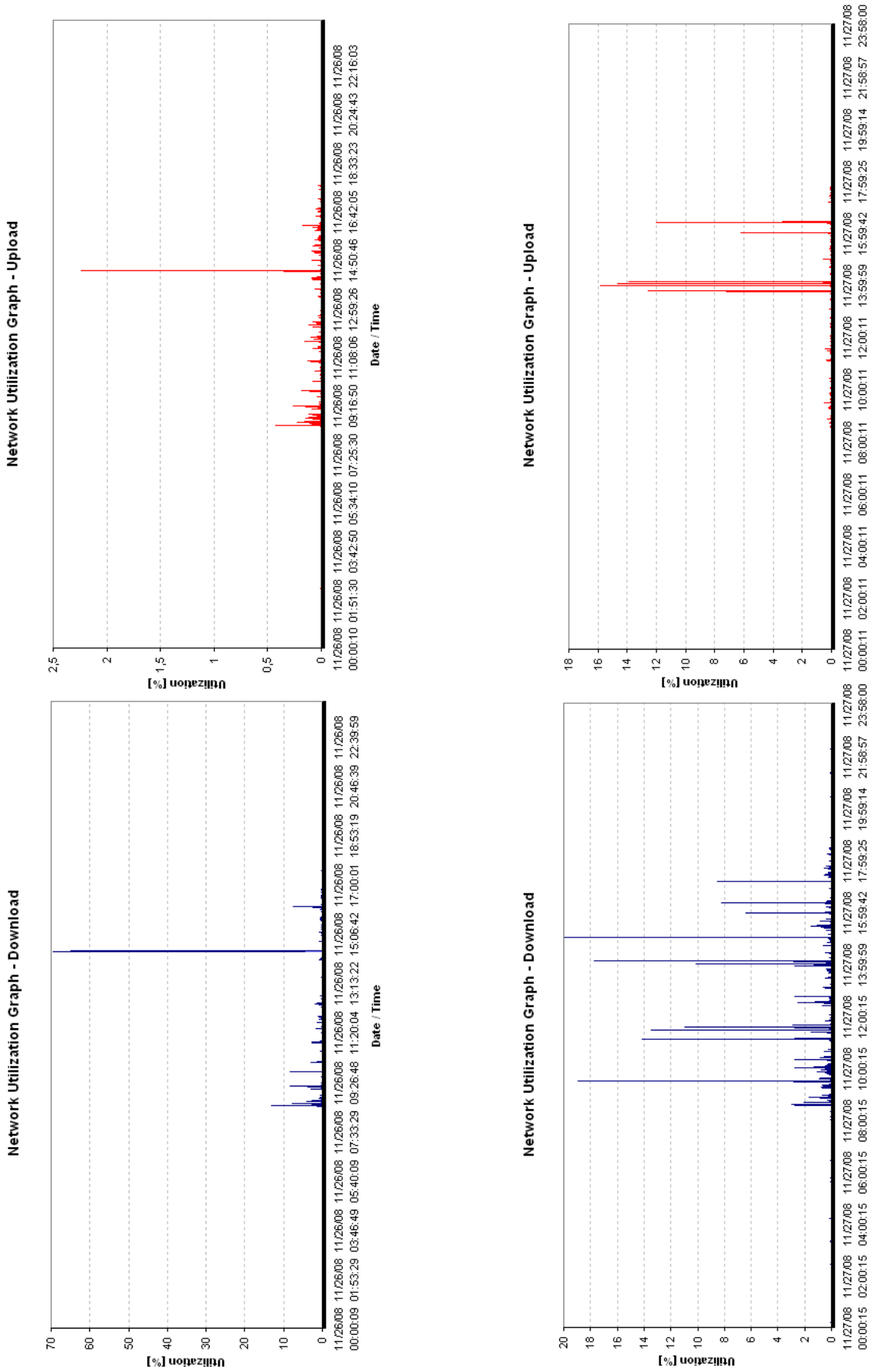
[18] MIKALSEN, A., BORGESEN, P.: *Local Area Network Management, Design & Security*. Chichester: John Wiley & Sons, 2002.

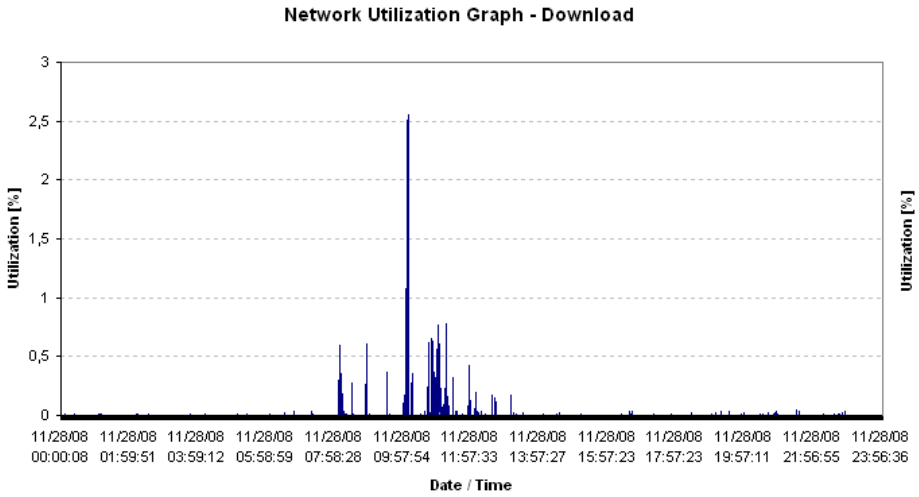
9. PŘEHLED POUŽITÝCH ZKRATEK

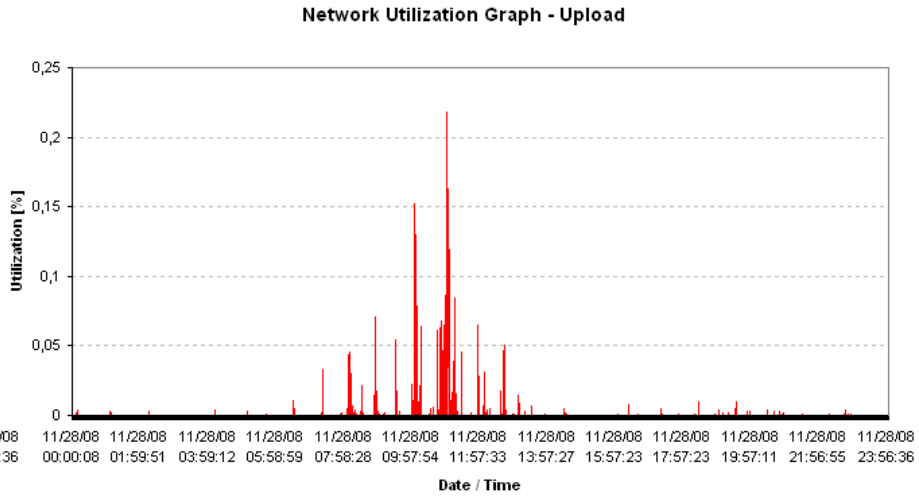
ACK	(Acknowledgment); příznak potvrzení v TCP
AP	(Access Point); přístupový bod
ARP	(Address Resolution Protocol); protokol pro překlad IP adres na MAC adresy
ASIC	(Application Specific Integrated Circuit); označení návrhu Finisar analyzátoru
BOOTP	(Bootstrap Protocol); protokol pro nastavení síťových parametrů
CRC	(Cycle Redundance Check); cyklický redundantní součet
DHCP	(Dynamic Host Configuration Protocol); protokol pro nastavení síťových parametrů
DNS	(Domain Name server); protokol pro převod IP adres na jména
FDDI	(Fiber Distributed Data Interface); označení sítě s kruhovou topologií
FIN	(Finalize); příznak konce spojení v TCP
FTP	(File Transport Protokol); souborový transportní protokol
HTTP	(Hyper Text Transfer Protokol); hypertextový protokol
ICMP	(Internet Control Message Protocol); komunikační protokol
IMAP	(Internet Message Access Protocol); protokol pro vzdálený přístup ke schránce elektronické pošty
IP	(Internet Protokol); internetový protokol
IPv4	(Internet Protokol version 4); IP protokol verze 4
IPv6	(Internet Protokol version 6); IP protokol verze 6
LAN	(Local Area Network); lokální počítačová síť
NTP	(Network Time Protocol); synchronizační protokol
OSI	(Open Systems Interconnection); propojení otevřených systémů
POP	(Post Office Protocol); protokol pro příjem elektronické pošty
PSH	(Push); push funkce v TCP
RARP	(Reverse Address Resolution Protocol); inverzní ARP
RST	(Reset); příznak resetování spojení v TCP
RTP	(Real-time Transfer Protocol); protokol pro přenosy v reálném čase
SMTP	(Simple Mail Transfer Protocol); protokol pro přenos zpráv elektronické pošty
SNMP	(Simple Network Management Protocol); protokol vzdálené správy
STP	(Shielded Twisted Pair); stíněná kroucená dvojlinka
SYN	(Synchronize); synchronizační sekvenční číslo v TCP
TCP	(Transmission Control Protocol); transportní protokol
TFTP	(Trivial File Transfer Protocol); protokol pro přenos souborů
TTL	(Time To Live); doba životnosti datagramu
UDP	(User Datagram Protocol); datagramový protokol
URG	(Urgent); příznak urgentní v TCP
UTP	(Unshielded Twisted Pair); nestíněná kroucená dvojlinka
VLAN	(Virtual Local Area Network); virtuální lokální síť
WAN	(Wide Area Network); rozsáhlá počítačová síť

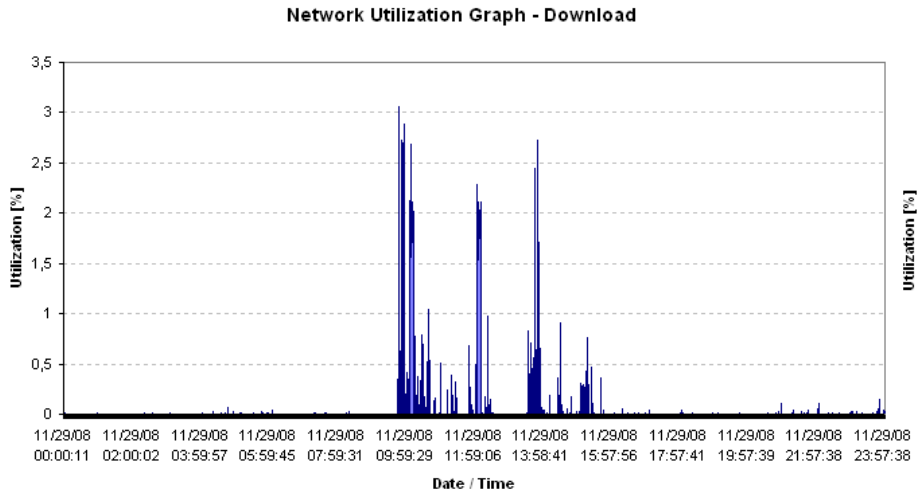
10.PŘÍLOHY

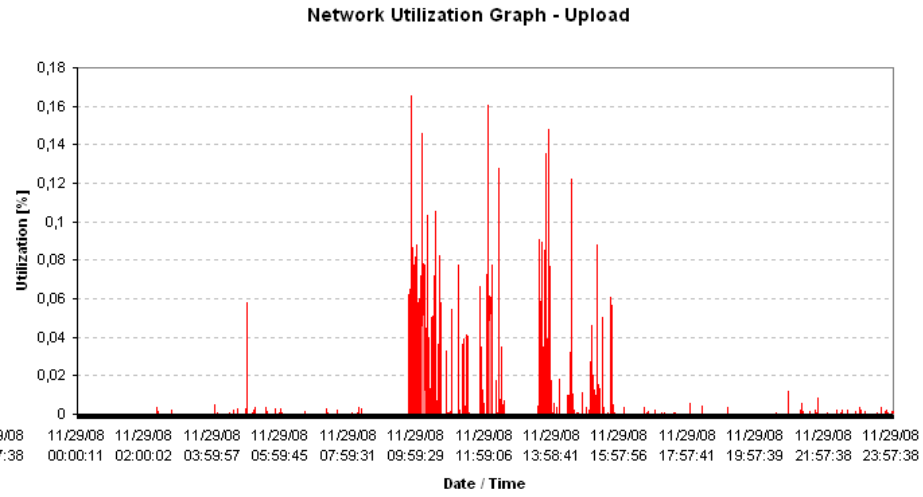
PŘÍLOHA 1: Zatížení sítě v obou směrech v jednotlivých dnech

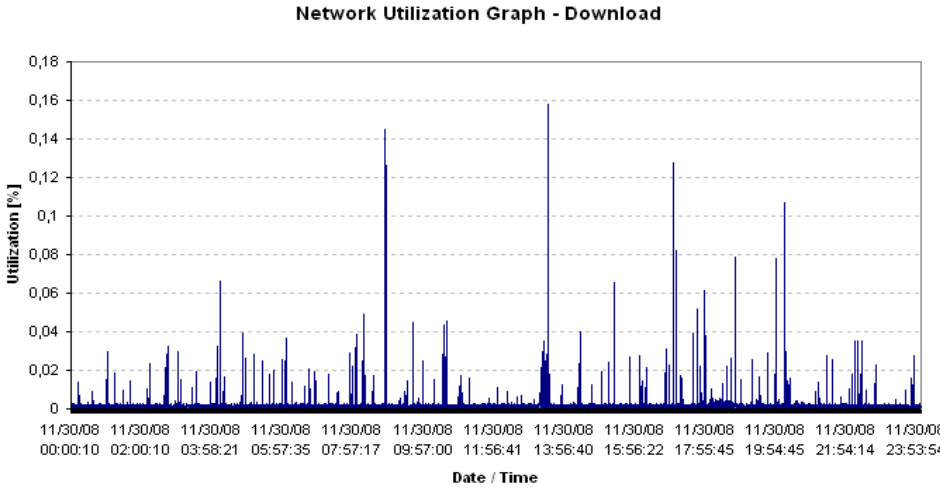


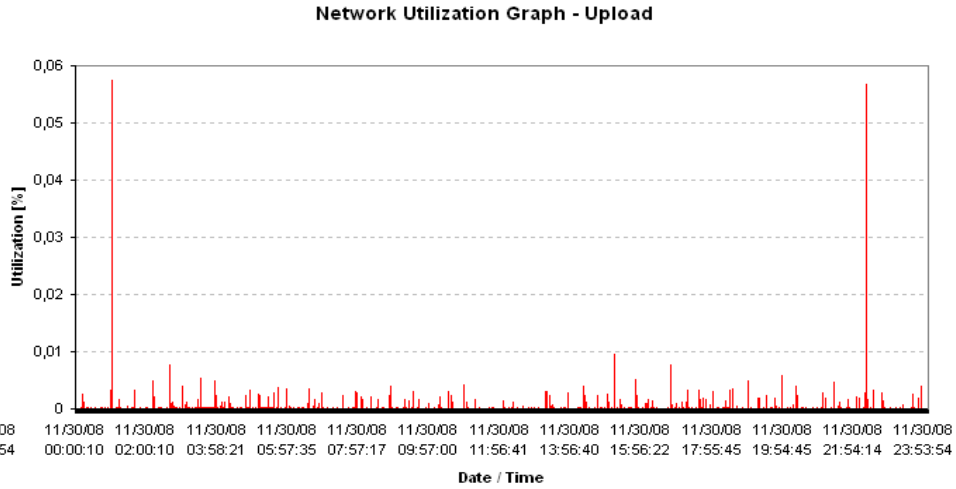

Network Utilization Graph - Download
Utilization [%]
3
2,5
2
1,5
1
0,5
0
11/28/08 00:00:08
11/28/08 01:59:51
11/28/08 03:59:12
11/28/08 05:58:59
11/28/08 07:58:28
11/28/08 09:57:54
11/28/08 11:57:33
11/28/08 13:57:27
11/28/08 15:57:23
11/28/08 17:57:23
11/28/08 19:57:11
11/28/08 21:56:55
11/28/08 23:56:36
Date / Time

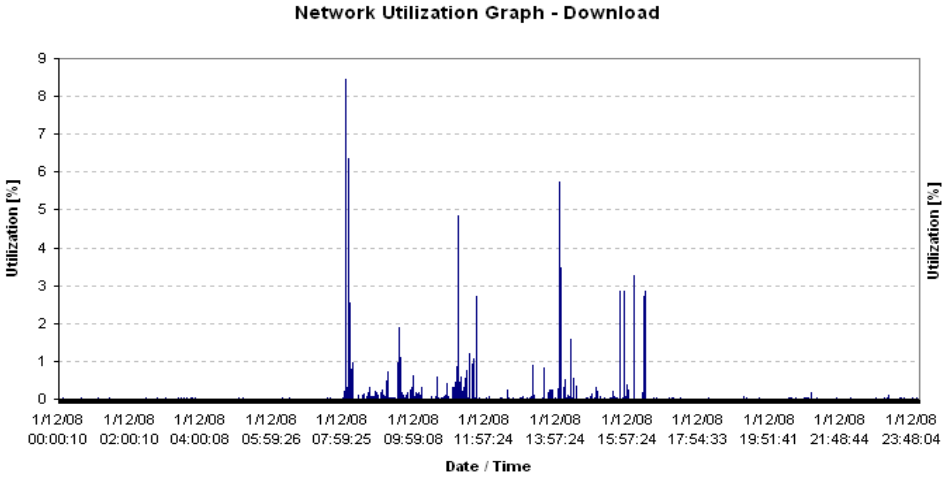

Network Utilization Graph - Upload
Utilization [%]
0,25
0,2
0,15
0,1
0,05
0
11/28/08 00:00:08
11/28/08 01:59:51
11/28/08 03:59:12
11/28/08 05:58:59
11/28/08 07:58:28
11/28/08 09:57:54
11/28/08 11:57:33
11/28/08 13:57:27
11/28/08 15:57:23
11/28/08 17:57:23
11/28/08 19:57:11
11/28/08 21:56:55
11/28/08 23:56:36
Date / Time

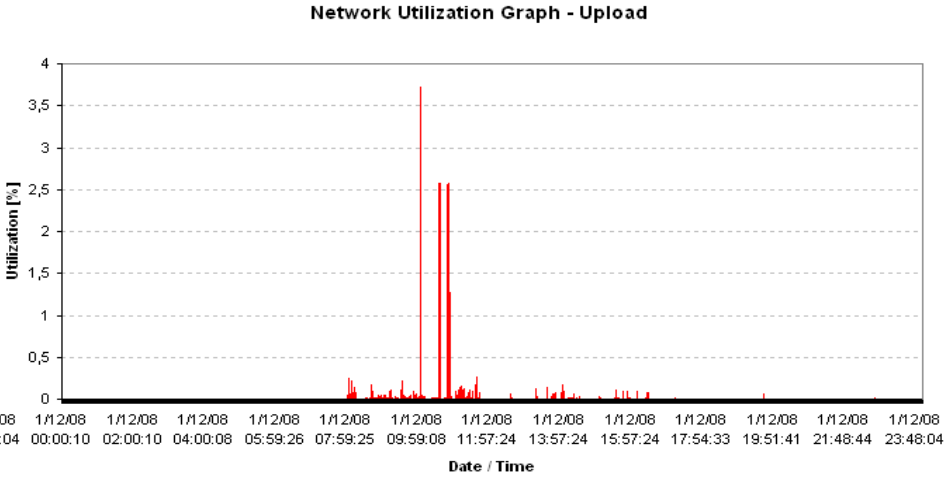

Network Utilization Graph - Download
Utilization [%]
3,5
3
2,5
2
1,5
1
0,5
0
11/29/08 00:00:11
11/29/08 02:00:02
11/29/08 03:59:57
11/29/08 05:59:45
11/29/08 07:59:31
11/29/08 09:59:29
11/29/08 11:59:06
11/29/08 13:58:41
11/29/08 15:57:56
11/29/08 17:57:41
11/29/08 19:57:39
11/29/08 21:57:38
11/29/08 23:57:38
Date / Time

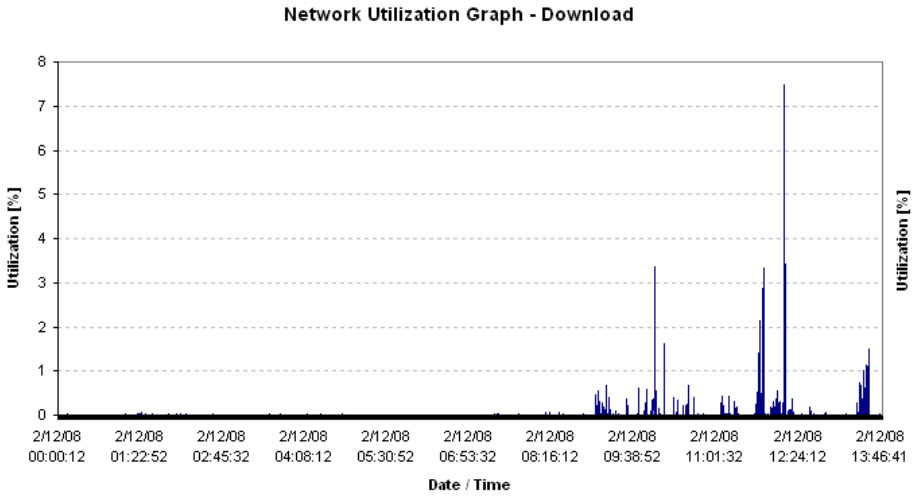

Network Utilization Graph - Upload
Utilization [%]
0,18
0,16
0,14
0,12
0,1
0,08
0,06
0,04
0,02
0
11/29/08 00:00:11
11/29/08 02:00:02
11/29/08 03:59:57
11/29/08 05:59:45
11/29/08 07:59:31
11/29/08 09:59:29
11/29/08 11:59:06
11/29/08 13:58:41
11/29/08 15:57:56
11/29/08 17:57:41
11/29/08 19:57:39
11/29/08 21:57:38
11/29/08 23:57:38
Date / Time

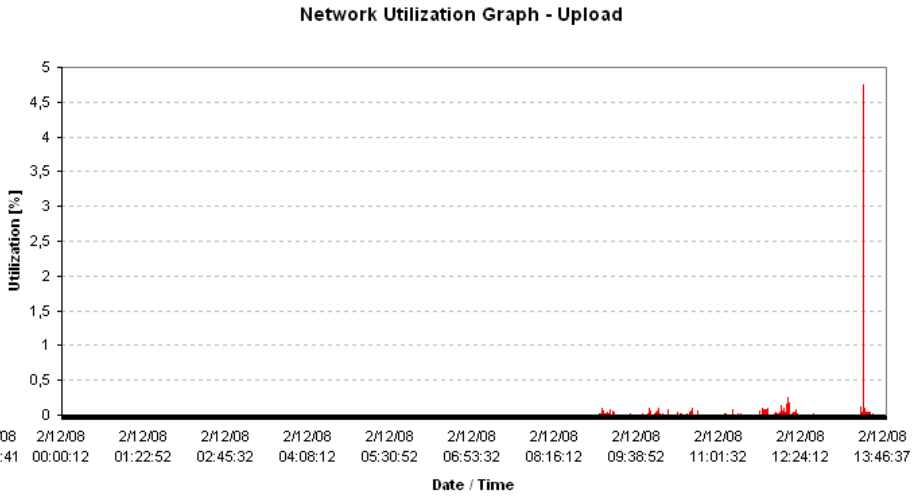

Network Utilization Graph - Download
Utilization [%]
0,18
0,16
0,14
0,12
0,1
0,08
0,06
0,04
0,02
0
11/30/08 00:00:10
11/30/08 02:00:10
11/30/08 03:58:21
11/30/08 05:57:35
11/30/08 07:57:17
11/30/08 09:57:00
11/30/08 11:56:41
11/30/08 13:56:40
11/30/08 15:56:22
11/30/08 17:55:45
11/30/08 19:54:45
11/30/08 21:54:14
11/30/08 23:53:54
Date / Time


Network Utilization Graph - Upload
Utilization [%]
0,06
0,05
0,04
0,03
0,02
0,01
0
11/30/08 00:00:10
11/30/08 02:00:10
11/30/08 03:58:21
11/30/08 05:57:35
11/30/08 07:57:17
11/30/08 09:57:00
11/30/08 11:56:41
11/30/08 13:56:40
11/30/08 15:56:22
11/30/08 17:55:45
11/30/08 19:54:45
11/30/08 21:54:14
11/30/08 23:53:54
Date / Time

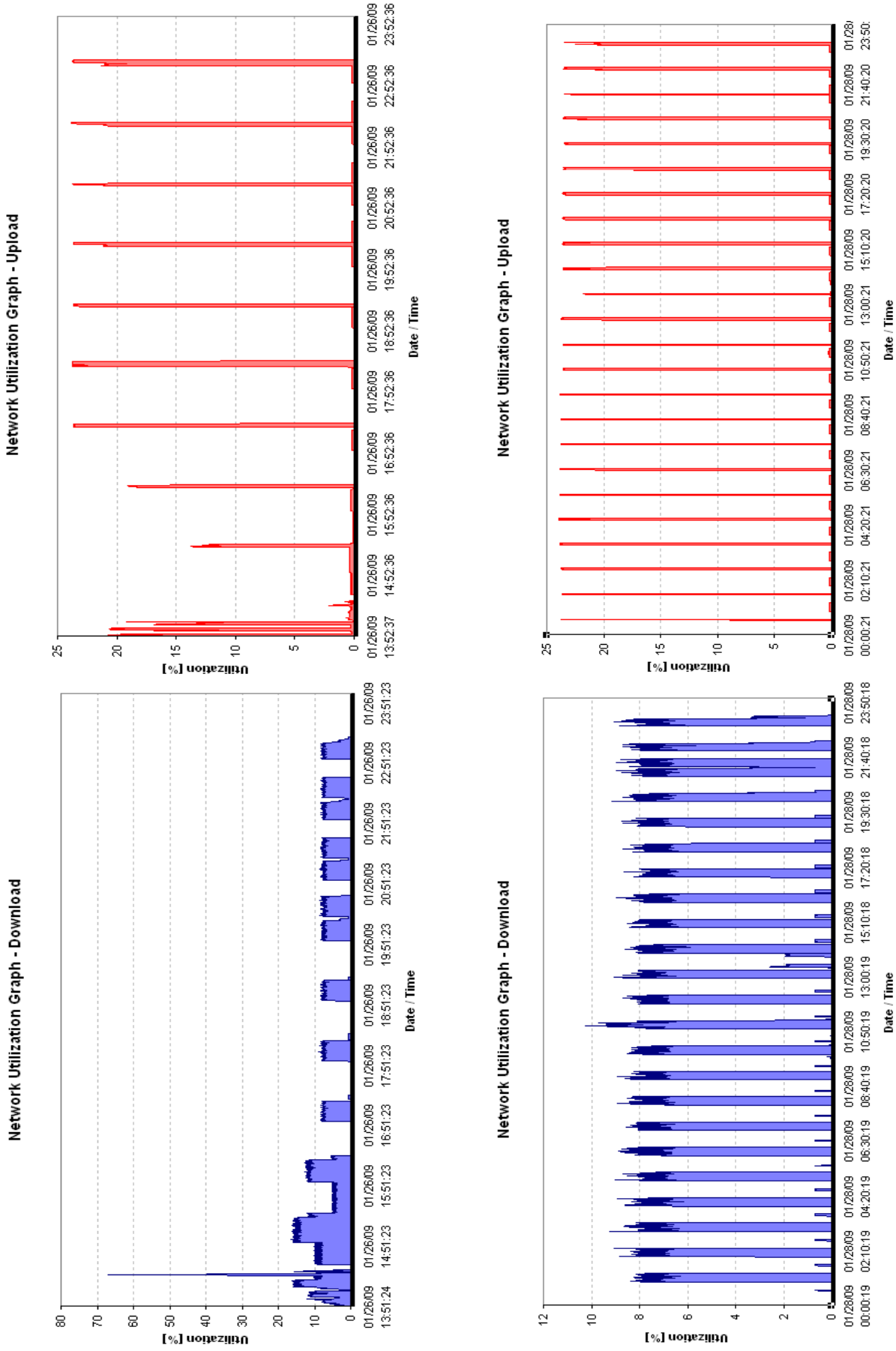

Network Utilization Graph - Download
Utilization [%]
9
8
7
6
5
4
3
2
1
0
1/12/08 00:00:10
1/12/08 02:00:10
1/12/08 04:00:08
1/12/08 05:59:26
1/12/08 07:59:25
1/12/08 09:59:08
1/12/08 11:57:24
1/12/08 13:57:24
1/12/08 15:57:24
1/12/08 17:54:33
1/12/08 19:51:41
1/12/08 21:48:44
1/12/08 23:48:04
Date / Time

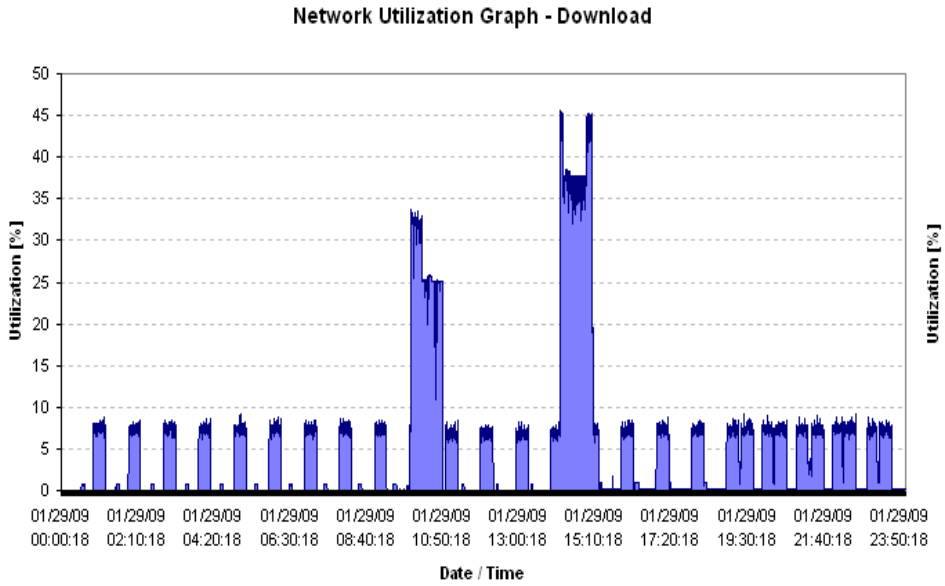

Network Utilization Graph - Upload
Utilization [%]
4
3,5
3
2,5
2
1,5
1
0,5
0
1/12/08 00:00:10
1/12/08 02:00:10
1/12/08 04:00:08
1/12/08 05:59:26
1/12/08 07:59:25
1/12/08 09:59:08
1/12/08 11:57:24
1/12/08 13:57:24
1/12/08 15:57:24
1/12/08 17:54:33
1/12/08 19:51:41
1/12/08 21:48:44
1/12/08 23:48:04
Date / Time

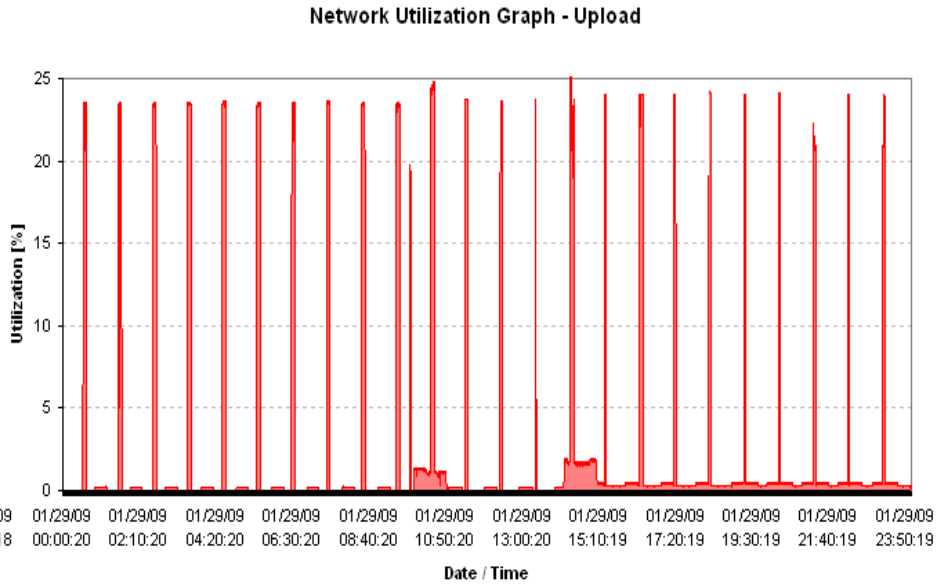

Network Utilization Graph - Download
Utilization [%]
0
1
2
3
4
5
6
7
8
2/12/08 00:00:12
2/12/08 01:22:52
2/12/08 02:45:32
2/12/08 04:08:12
2/12/08 05:30:52
2/12/08 06:53:32
2/12/08 08:16:12
2/12/08 09:38:52
2/12/08 11:01:32
2/12/08 12:24:12
2/12/08 13:46:41
Date / Time

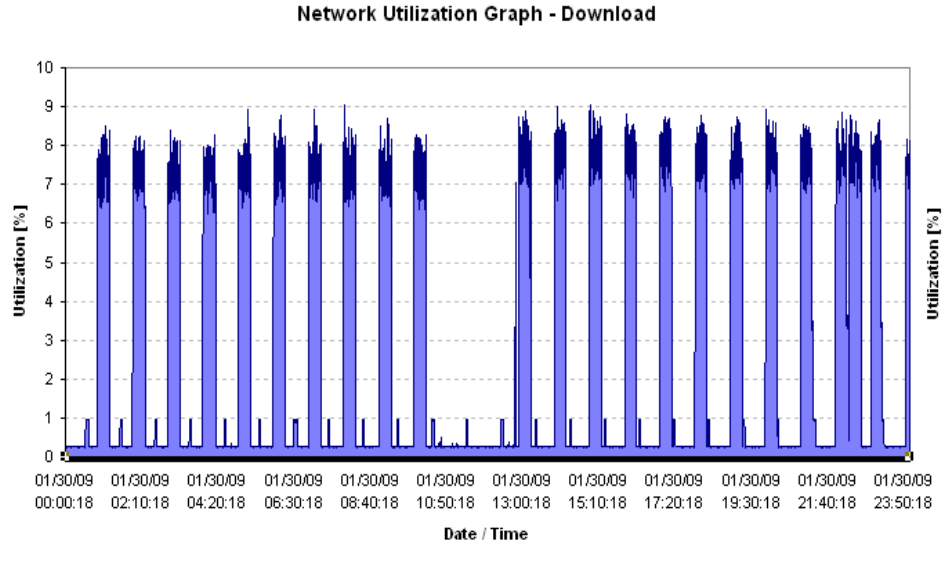

Network Utilization Graph - Upload
Utilization [%]
0
0,5
1
1,5
2
2,5
3
3,5
4
4,5
5
2/12/08 00:00:12
2/12/08 01:22:52
2/12/08 02:45:32
2/12/08 04:08:12
2/12/08 05:30:52
2/12/08 06:53:32
2/12/08 08:16:12
2/12/08 09:38:52
2/12/08 11:01:32
2/12/08 12:24:12
2/12/08 13:46:37
Date / Time

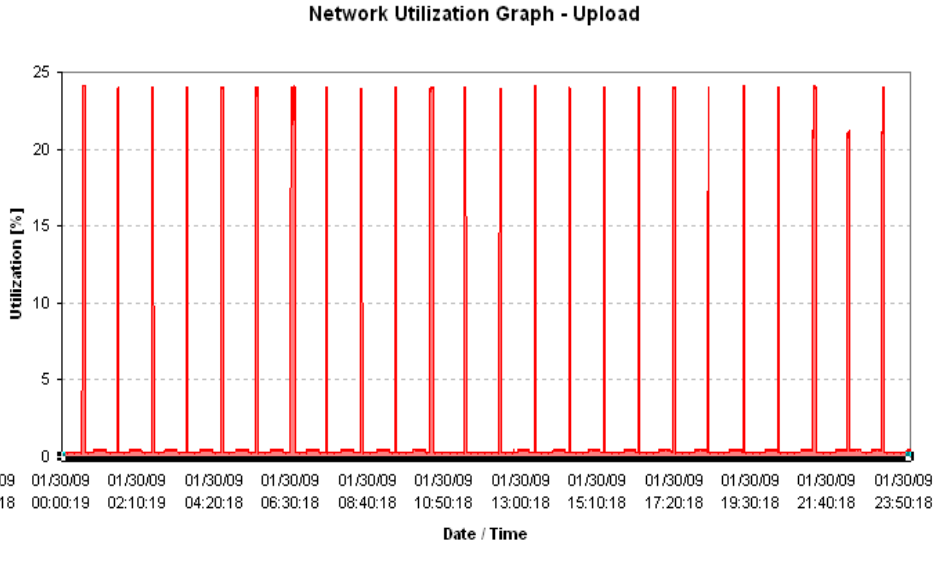
PŘÍLOHA 2: Zatížení sítě v obou směrech pro jednotlivé dny II. monitorování

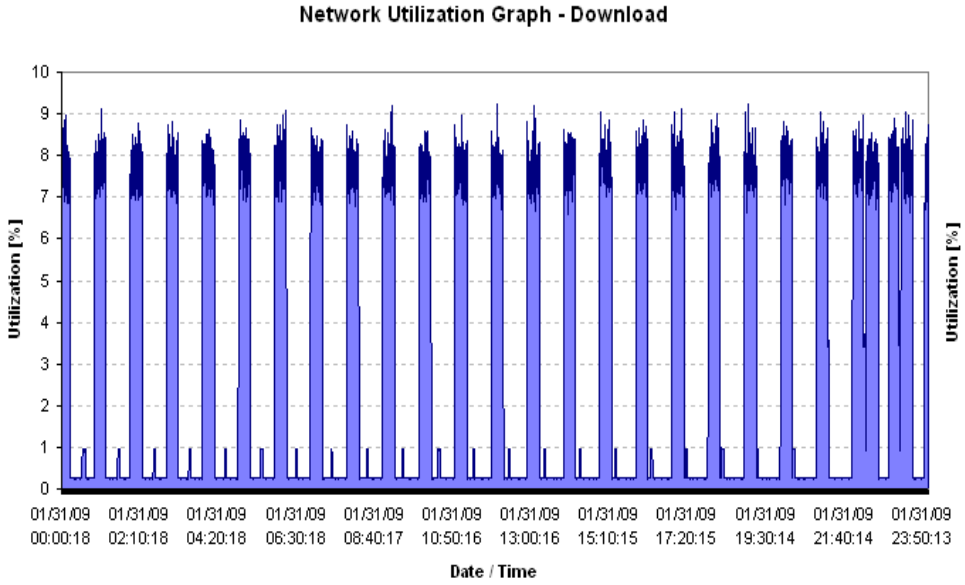


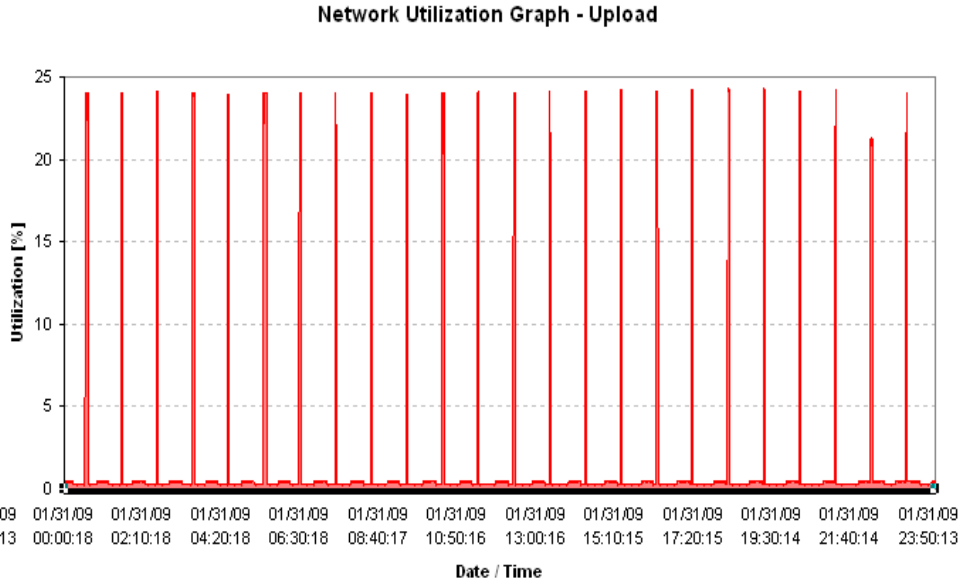

Network Utilization Graph - Download
Utilization [%]
50
45
40
35
30
25
20
15
10
5
0
01/29/09 00:00:18
01/29/09 02:10:18
01/29/09 04:20:18
01/29/09 06:30:18
01/29/09 08:40:18
01/29/09 10:50:18
01/29/09 13:00:18
01/29/09 15:10:18
01/29/09 17:20:18
01/29/09 19:30:18
01/29/09 21:40:18
01/29/09 23:50:18
Date / Time

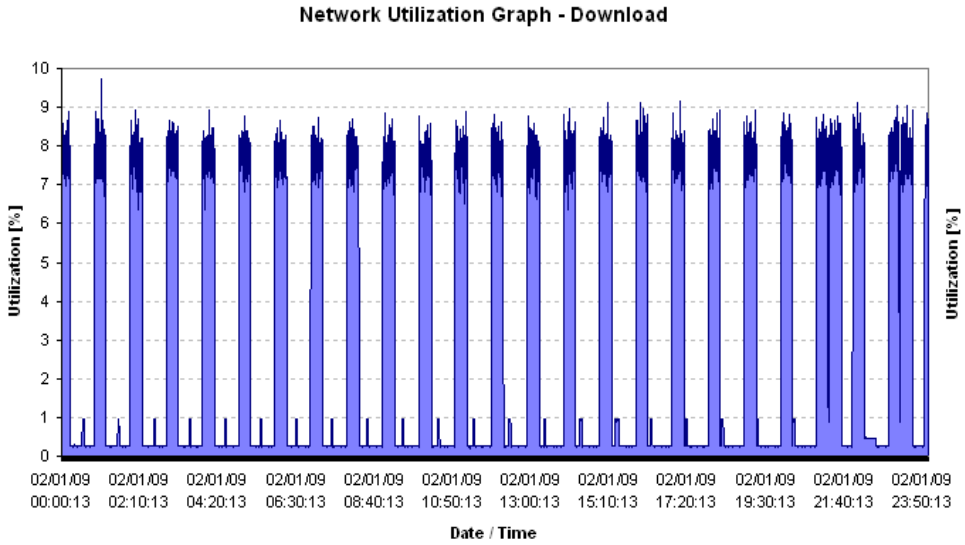

Network Utilization Graph - Upload
Utilization [%]
25
20
15
10
5
0
01/29/09 00:00:20
01/29/09 02:10:20
01/29/09 04:20:20
01/29/09 06:30:20
01/29/09 08:40:20
01/29/09 10:50:20
01/29/09 13:00:20
01/29/09 15:10:19
01/29/09 17:20:19
01/29/09 19:30:19
01/29/09 21:40:19
01/29/09 23:50:19
Date / Time

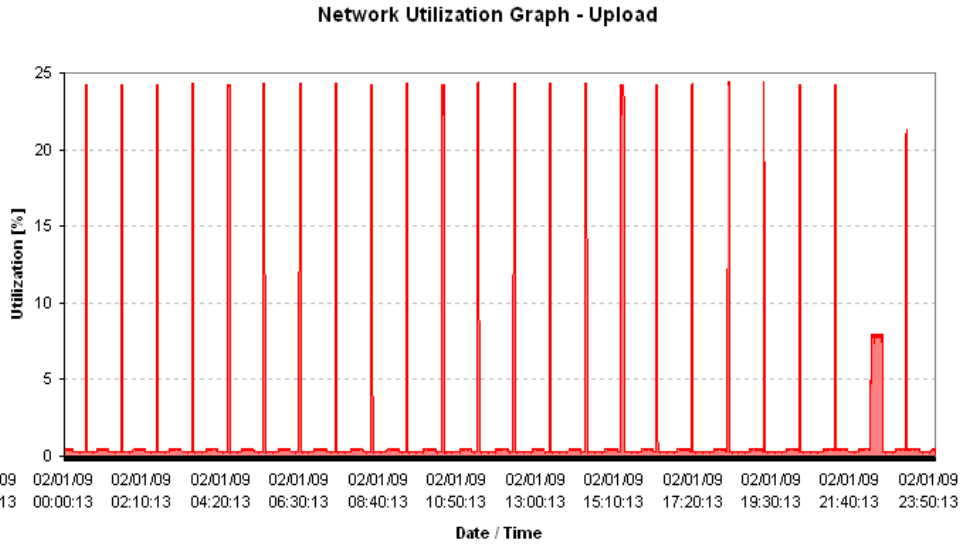

Network Utilization Graph - Download
Utilization [%]
10
9
8
7
6
5
4
3
2
1
0
01/30/09 00:00:18
01/30/09 02:10:18
01/30/09 04:20:18
01/30/09 06:30:18
01/30/09 08:40:18
01/30/09 10:50:18
01/30/09 13:00:18
01/30/09 15:10:18
01/30/09 17:20:18
01/30/09 19:30:18
01/30/09 21:40:18
01/30/09 23:50:18
Date / Time

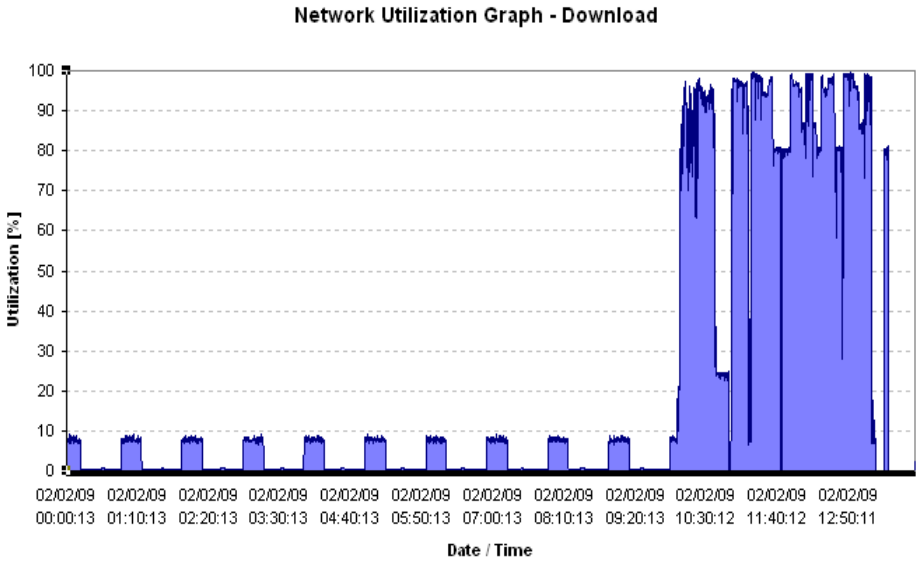

Network Utilization Graph - Upload
Utilization [%]
25
20
15
10
5
0
01/30/09 00:00:19
01/30/09 02:10:19
01/30/09 04:20:18
01/30/09 06:30:18
01/30/09 08:40:18
01/30/09 10:50:18
01/30/09 13:00:18
01/30/09 15:10:18
01/30/09 17:20:18
01/30/09 19:30:18
01/30/09 21:40:18
01/30/09 23:50:18
Date / Time

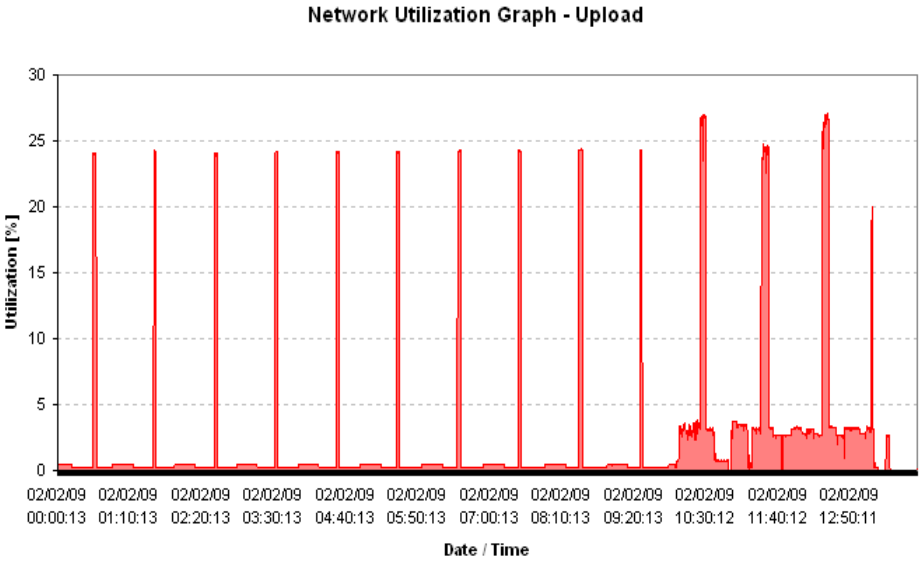

Network Utilization Graph - Download
Utilization [%]
0
1
2
3
4
5
6
7
8
9
10
01/31/09 00:00:18
01/31/09 02:10:18
01/31/09 04:20:18
01/31/09 06:30:18
01/31/09 08:40:17
01/31/09 10:50:16
01/31/09 13:00:16
01/31/09 15:10:15
01/31/09 17:20:15
01/31/09 19:30:14
01/31/09 21:40:14
01/31/09 23:50:13
Date / Time


Network Utilization Graph - Upload
Utilization [%]
0
5
10
15
20
25
01/31/09 00:00:18
01/31/09 02:10:18
01/31/09 04:20:18
01/31/09 06:30:18
01/31/09 08:40:17
01/31/09 10:50:16
01/31/09 13:00:16
01/31/09 15:10:15
01/31/09 17:20:15
01/31/09 19:30:14
01/31/09 21:40:14
01/31/09 23:50:13
Date / Time


Network Utilization Graph - Download
Utilization [%]
0
1
2
3
4
5
6
7
8
9
10
02/01/09 00:00:13
02/01/09 02:10:13
02/01/09 04:20:13
02/01/09 06:30:13
02/01/09 08:40:13
02/01/09 10:50:13
02/01/09 13:00:13
02/01/09 15:10:13
02/01/09 17:20:13
02/01/09 19:30:13
02/01/09 21:40:13
02/01/09 23:50:13
Date / Time


Network Utilization Graph - Upload
Utilization [%]
0
5
10
15
20
25
02/01/09 00:00:13
02/01/09 02:10:13
02/01/09 04:20:13
02/01/09 06:30:13
02/01/09 08:40:13
02/01/09 10:50:13
02/01/09 13:00:13
02/01/09 15:10:13
02/01/09 17:20:13
02/01/09 19:30:13
02/01/09 21:40:13
02/01/09 23:50:13
Date / Time


Network Utilization Graph - Download
Utilization [%]
100
90
80
70
60
50
40
30
20
10
0
02/02/09 00:00:13
02/02/09 01:10:13
02/02/09 02:20:13
02/02/09 03:30:13
02/02/09 04:40:13
02/02/09 05:50:13
02/02/09 07:00:13
02/02/09 08:10:13
02/02/09 09:20:13
02/02/09 10:30:12
02/02/09 11:40:12
02/02/09 12:50:11
Date / Time


Network Utilization Graph - Upload
Utilization [%]
30
25
20
15
10
5
0
02/02/09 00:00:13
02/02/09 01:10:13
02/02/09 02:20:13
02/02/09 03:30:13
02/02/09 04:40:13
02/02/09 05:50:13
02/02/09 07:00:13
02/02/09 08:10:13
02/02/09 09:20:13
02/02/09 10:30:12
02/02/09 11:40:12
02/02/09 12:50:11
Date / Time